Ministério da Justiça

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Relatório Parcial de Entrega do Projeto

Documento:

RT Proteção de Template Biométrico

Data de Emissão:

07/07/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Helvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
José Carneiro da Cunha Oliveira Neto
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
09/03/2015	0.1	Primeira versão de apresentação do Relatório Parcial.
07/07/2015	0.1.1	Versão revisada.

latitude
Laboratório de tecnologias da tomada de decisão
B
Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

SUMÁRIO

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

1 INTRODUÇÃO

Em uma iniciativa de identificação civil, diversos questionamentos e dificuldades surgem naturalmente. Um problema central é como fazê-la. A resposta mais comum atualmente está na utilização de características biométricas das pessoas para individualizá-las. Porém, a segurança na atividade de individualização dos cidadãos é um exemplo de dificuldade relevante nesse processo, já que o sucesso de algum indivíduo malicioso em se passar por outra pessoa compromete o requisito fundamental de não-repúdio da função de autenticação que um sistema de gerenciamento de identidades biométricas deve possuir.

Geralmente, deseja-se confiar em quem o sistema de identificação biométrica reconhece, não significando que o indivíduo não reconhecido seja necessariamente impostor, ou que o reconhecido seja realmente genuíno. A performance de um sistema biométrico é dada pela relação entre as taxas de erro dessas falhas. A intenção ao se projetar um sistema biométrico de identificação é obter as menores taxas de erro possíveis.

Os códigos corretores de erro utilizados na obtenção e na comparação dos dados biométricos são as principais ferramentas na construção de um sistema biométrico eficiente. Contudo, não há códigos capazes de garantir comparações exatas e sem falhas entre amostras biométricas. Como se trata de uma característica biológica ou comportamental, a presença de ruído na coleta desses dados é intrínseca, seja por conta do sensor de detecção, seja por modificações comportamentais ou fisiológicas ocorridas naturalmente com o decorrer do tempo.

Mais ainda, quanto melhor a correção de erro de um código, pior o seu desempenho em termos do tempo de comparação, o que se agrava quando há a necessidade de identificar uma amostra biométrica em grandes bases de dados, típicas de sistemas de identificação civil nacionais. Cabe ressaltar que o foco dessa pesquisa não é o uso da proteção de *template* biométrico para identificação em bases biométricas anônimas, e sim para a proteção do *template* biométrico usado na verificação. Além disso, para uma comparação entre dados biométricos mais exata, sacrifica-se boa parte da entropia resultante do *template* [14]. Outra externalidade negativa relevante é a possibilidade de vazamento de informação sobre o dado biométrico por meio dos dados auxiliares gerados por códigos corretores de erro em sistemas gestores de *templates* biométricos.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Por conta disso, é inevitável que os sistemas biométricos confundam amostras de diferentes pessoas, podendo ocorrer a falsa aceitação assim como a falsa rejeição de uma tentativa de autenticação. O compromisso comumente estabelecido nessa situação é a escolha de um limiar que estabeleça o percentual aceitável de erro do sistema. Caso seja inadmissível a aceitação de um impostor, o limiar a ser escolhido será tal que a probabilidade de falsas rejeições ocorrerem crescerá. Em processos criminais, a criticidade da análise é maior, pois o réu só deve ser condenado se, por exemplo, as impressões digitais encontradas na cena do crime forem atribuídas a ele com um nível mínimo de certeza. Isso impõe ao sistema de identificação biométrica a necessidade de elevada certeza na identificação do suspeito, como uma baixa taxa de falso positivo. Logo, o limiar deverá ser tal que um inocente não possa ser identificado como autor de um crime. Esse ajuste, entretanto, eleva a taxa de falso negativos e abre margem para que muitos criminosos sejam inocentados por falta de provas, já que podem ser falsamente rejeitados na identificação biométrica, em prol da garantia de não se condenar um inocente.

Segurança talvez seja o requisito mais relevante na identificação civil. O problema é que definir segurança não é tarefa fácil. Muitos aspectos conflitantes estão envolvidos nessa tarefa, o que impõe uma relação de compromisso entre muitas escolhas. O melhor exemplo disso é justamente o uso de biometria para se garantir a segurança na identificação de um indivíduo. Há muitas possibilidades de vazamento da privacidade dos dados biométricos de uma pessoa, seja por meio de ataques às bases de dados, seja através de equipamentos sensores adulterados, seja pela cópia obtida a partir do próprio documento de identificação ou da obtenção de uma imagem da biometria da pessoa. Tantos são os cenários que não há como esgotá-los aqui. A segurança de um sistema está justamente em evitar possíveis vazamentos desses dados. Porém, mais do que isso, um sistema realmente seguro deve impedir que um indivíduo malicioso que tenha se apoderado de dados biométricos de terceiros seja capaz de se autenticar genuinamente, se passando por outra pessoa.

O uso de técnicas criptográficas para essa finalidade tem sido muito difundido. Embora ainda não esteja disponível no mercado um sistema inviolável, a mitigação dos riscos e ataques de segurança pode ser obtida em níveis aceitáveis com a tecnologia disponível. Resultados recentes, porém ainda acadêmicos, apresentam soluções

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

promissoras para as questões envolvendo a segurança de *templates* armazenados em bases de dados governamentais, em cartões com memória ou mesmo impressas em papel moeda. De qualquer forma, a escolha de padrões de mercado atuais não afeta a possibilidade de se adotar soluções mais seguras no futuro. Importante é estabelecer um modelo que facilite a troca dos padrões utilizados sem implicar em grandes custos, mudanças trabalhosas ou necessidade de mobilizações em massa.

Essas são algumas das preocupações enfrentadas pela equipe do Projeto de Identificação Civil Única – RIC – do Ministério da Justiça. A finalidade desse trabalho é auxiliar na tomada de decisão sobre as técnicas, algoritmos e protocolos adequados a serem adotados para elaborar e disponibilizar um documento de identificação seguro à população, que disponibilize um método de verificação presencial confiável e permita a identificação de forma ágil, simples e segura do cidadão, a fim de desburocratizar o acesso aos serviços governamentais e comerciais necessários à vida diária de todos, diminuindo drasticamente o número de fraudes existentes atualmente.

1.1 Objetivo

A finalidade desse relatório parcial é sugerir recomendações para os seguintes questionamentos sobre segurança envolvendo a proteção de *templates* biométricos, conforme estabelecido no Dicionário de EAP do Projeto RIC elaborado para o 2º Semestre de 2014.

- Qual das biometrias indicadas para utilização na identificação civil única no Brasil é mais adequada para a verificação biométrica com proteção de *template*, considerando os respectivos algoritmos de coleta dessas biometrias, a performance, as taxas de distribuição de erros e a entropia do *template* biométrico obtido da aplicação dos respectivos algoritmos.
- Quais códigos corretores de erro permitem comparação exata de *template* biométrico e qual o resultado da análise de performance deles em relação a entropia resultante e o tempo de execução da comparação.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

- Quais os esquemas criptográficos disponíveis na literatura para proteger o *template* biométrico e como usá-los para fortalecer a autenticação com uso de outros fatores, como chave privada, *token* ou senha.
- Quais as premissas de segurança e os possíveis ataques que resultem em vazamento dos dados biométricos e possíveis soluções de revogabilidade do *template*, como forma de contornar essa fragilidade.
- Qual a viabilidade de um esquema de gravação do *template* biométrico no documento de identificação, seja impresso em papel ou armazenado em cartão de policarbonato com chip de memória e processamento.
- Estudo sobre os possíveis modelos de autenticação biométrica, com autenticação passiva dos dados e com o uso de cartão com memória com autenticação ativa do *chip*.
- Estudo sobre os possíveis ataques como substituição parcial ou total dos dados.
- Especificação do algoritmo de geração do *template* biométrico para comparação exata.
- Especificação do processo de verificação do *template* biométrico, com emprego de outros fatores de autenticação como senha ou chave privada, caso seja aplicado.
- Relatório conclusivo contendo os estudos e recomendações sobre as tecnologias disponíveis, análise de custo/benefício e indicação de um modelo seguro.

Pode-se observar que os questionamentos são abordados apenas nos 5 primeiros quesitos acima, já que os demais constituem estudos, especificações e elaboração de relatório, que são contemplados em parte com a própria apresentação do presente trabalho, principalmente nos capítulos de Revisão Bibliográfica e de Conceitos e Definições.

Importante destacar que os objetivos traçados não serão atendidos completamente nesta versão parcial do relatório. Isso porque atacar cada um desses objetivos de forma definitiva exige uma vasta pesquisa, com a elaboração de estudos sobre desempenho comparado entre os protocolos e prospecções das soluções de mercado. Assim, as recomendações feitas aqui têm caráter preliminar, baseadas em uma avaliação subjetiva, mas fundamentadas nos conhecimentos e nas experiências anteriores deste autor no tratamento de temas relacionados à segurança da informação, criptografia e biometria. As respostas formais, com fundamentos sólidos e referenciados em uma revisão bibliográfica

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

exaustiva e baseados em dados oficiais e pesquisas científicas realizadas tanto pelo autor quanto pelo grupo que compõe a área de pesquisa do projeto serão apresentadas em um possível estudo futuro a ser apresentado em versão definitiva do relatório.

1.2 Organização

Este relatório está organizado da seguinte forma. No capítulo 2 é realizada uma revisão bibliográfica da literatura sobre segurança biométrica. O capítulo 3 é dedicado à sugestão e indicação de recomendações às indagações e demandas elencadas nos objetivos do projeto, com foco nos tópicos do Dicionário de EAP de 2014. Por fim, o capítulo 4 traz a conclusão parcial com uma resposta concisa à dúvida central em tela, sobre a viabilidade de se proteger de forma segura o *template* biométrico armazenado em documentos de identificação civil.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

2 REVISÃO BIBLIOGRÁFICA

2.1 Contextualização

Atualmente, cada vez mais órgãos públicos e empresas privadas têm investido em Sistemas de Autenticação Eletrônica com a finalidade de identificação segura de seus funcionários. O uso de tecnologia baseada na biometria cresceu rapidamente nesses sistemas [1]. Entretanto, o uso de biometria está inevitavelmente associado a questões de privacidade e segurança [2] [3]. O dado biométrico, que é armazenado em um *smart card* ou em uma base de dados central, apresenta um risco de vazamento devido ao aumento do número de ataques a sistemas de gerenciamento de identidade nos últimos anos [2] [3] [4] [5].

As preocupações com a segurança e a privacidade do dado biométrico limitam o seu uso disseminado em diversas aplicações no mundo real. A primeira solução que vem em mente para solução dos problemas de segurança e de privacidade é o uso de primitivas criptográficas. Porém, não é possível aplicar diretamente aos *templates* biométricos as técnicas e ferramentas criptográficas convencionais, como AES ou TLS, já que os dados biométricos são intrinsecamente ruidosos [6]. Ou seja, o sensor de coleta biométrica, mesmo sendo utilizado várias vezes por um mesmo indivíduo, não consegue gerar exatamente o mesmo dado biométrico repetidamente. Com isso, o *template* biométrico que é armazenado de modo criptografado precisa ser decifrado para a realização da comparação com a amostra gerada na fase de verificação. Logo, devido à necessidade de se decifrar o *template,* fica-se sujeito novamente ao vazamento de privacidade e às brechas de segurança [6].

Cabe ressaltar que a norma ISO/IEC 24745 propõe um modelo referencial de sistemas de proteção de *template* biométrico, elencando diversas opções de métodos, mas não prevê o uso unicamente de criptografia clássica da informação biometria com uso de chave secreta [7]. Os problemas do uso único de esquemas criptográficos de chave para proteção da biometria serão abordados em [8].

Outro problema relacionado ao uso direto de criptografia como solução é o gerenciamento de chave, principalmente quanto ao armazenamento das chaves criptográficas. Quando um administrador de uma base de dados se comporta maliciosamente e obtém as chaves, ele pode decifrar a informação armazenada no banco e obter os *templates* de cada usuário. Problema parecido ocorre com o uso de funções de *hash*. Uma vez que o *hash*

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

criptográfico é uma função *one-way,* quando um simples bit é alterado o resultado do *hash* se torna completamente diferente, devido ao efeito avalanche [9]. Então, a autenticação bem-sucedida por meio de comparação exata não pode ser realizada trivialmente mesmo no caso de um indivíduo legítimo, por conta do ruído natural existente em dados biométricos.

Sistemas biométricos que fazem uso de códigos corretores de erro foram propostos para lidar com o ruído intrínseco existente nesses dados [10] [11] [12]. Nesses sistemas, o dado biométrico coletado na fase de registro é exatamente o mesmo daquele obtido com a amostra na fase de verificação, já que os códigos mapeiam a informação ruidosa sempre para uma mesma palavra código, caso a capacidade de correção do código seja superior ao erro provocado pelo ruído. Assim, esses sistemas podem obter *templates* biométricos livres de erro, apropriados à aplicação de algoritmos criptográficos padrões, como funções de *hash*, sem sofrerem do efeito avalanche [12] [13] [14].

Entretanto, esses requisitos de elevada capacidade de correção de erro tornam inviáveis sua utilização na prática, no caso de aplicações reais, devido à grande redução na entropia do *template* e do baixo desempenho do sistema [15]. Além disso, a informação auxiliar gerada pelos esquemas de correção de erros pode vazar a informação sobre o *template* biométrico por meio de análises estatísticas [16]. Zhou et al. demonstraram de forma contundente em trabalho realizado que a redundância usada em códigos corretores de erro provoca o comprometimento da privacidade em sistemas biométricos [17] [18].

Embora esquemas criptográficos de proteção do *template* biométrico tenham sido propostos para superar os problemas de segurança e privacidade biométricos [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29], pesquisas recentes mostram que esses esquemas ainda apresentam falhas de segurança [30] [31] [32] [33] [34] [35] [36], e que tentativas de personificação, que é a capacidade de se passar por outra pessoa por meio de recursos forjados, são facilmente simuladas com sucesso [37] [38] [39]. Além disso, há um grande número de trabalhos sobre vazamento de privacidade em aplicações de criptossistemas biométricas [40] [41], e mais ainda no caso de métodos de proteção criptográfica de *template* biométrico [42] [17] [18]

Na literatura da área, em um importante trabalho, Zhou et al. propuseram um modelo criptográfico para a análise de segurança e de privacidade de métodos de proteção de *template* biométrico [17]. Em outro trabalho, Ignatenko et al. analisaram o vazamento de

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

privacidade em termos de informação mútua entre os dados auxiliares públicos, utilizados para auxiliar a atividade de verificação, e as informações sobre a biometria a ser protegida- nos sistemas criptográficos de proteção de *templates.* Uma relação de compromisso entre a taxa de segredo gerado com base na informação biométrica disponível e a taxa de vazamento de privacidade do *template* produzido foi estabelecida em [41] [43]. Assim, os autores apresentam resultados teóricos sólidos que demonstram a relação de vazamento de informação da biometria original do indivíduo tanto em sistemas biométricos que produzem chaves a partir do dado biométrico quanto em sistemas que utilizam chaves secretas aleatórias para protegerem o dado biométrico.

Recentemente, métodos de criptografia homomórfica foram usados em conjunto com métodos de extração das características biométricas para realizar a verificação por meio de operações sobre *templates* biométricos cifrados [20] [44] [45] [46]. Entretanto, esses métodos são baseados apenas no modelo de segurança honesto-porém-curioso, onde cada participante é obrigado a seguir o protocolo, embora possa realizar qualquer computação sobre os dados aprendidos durante a execução do protocolo para tentar obter informação adicional. Os métodos existentes não foram projetados para resistirem ao cenário do adversário malicioso, onde cada participante pode se desviar arbitrariamente do protocolo e se corromper.

Outro aspecto relevante é que tais métodos não levaram em conta a segurança e a privacidade dos dados biométricos armazenados na base de dados central [20] [46]. Os autores afirmam que o modelo de segurança que propõem será aperfeiçoado em trabalhos futuros por meio da utilização de protocolos criptográficos para cifrar os dados biométricos armazenados na base de dados, mas tal abordagem é inadequada, conforme análise acima. Fora isso, alguns desses sistemas foram projetados para lidar apenas com o uso de uma única modalidade biométrica ou até mesmo aspectos específicos de metodologias de extração de minúcias da biometria, o que limita sobremaneira a aplicabilidade desses sistemas [44] [45]. Ainda há a possibilidade de o adversário se registrar no lugar de qualquer outro indivíduo nesses sistemas, já que eles não oferecem qualquer tratamento para o ataque de personificação, no qual um impostor se passa por uma parte legítima com sucesso fraudando algum recurso do sistema ou forjando alguma característica de outro indivíduo. Finalmente, todos esses sistemas sofrem de elevada complexidade computacional, o que degradaria significativamente a performance de aplicações práticas baseadas neles.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

O esquema de *Biohashing* é uma técnica emergente, inicialmente aplicada à biometria da face e usando um esquema de regeneração de chave em conjunto com transformações reversíveis com uso de chave [47]. Este esquema e suas variantes tem sido muito estudada nos últimos tempos [25] [26] [27] [28] [29]. Esse esquema apresenta baixa taxa de erro e rápido desempenho na etapa de verificação da biometria. Entretanto, este método e suas variantes são suscetíveis a diversos ataques relatados na literatura [33] [34] [35] [36]. Para ser usado em aplicações práticas com segurança, esse esquema necessita de aperfeiçoamento. Há trabalhos que atuam nesse sentido [48], com a proposta de um novo protocolo de registro e verificação seguros para qualquer característica biométrica que possa ser transformada em *templates* na forma de *strings* binárias, mesmo no caso de multibiometrias. Mas esse ainda é um trabalho que está em desenvolvimento no âmbito acadêmico, sem disponibilidade no mercado.

2.2 Trabalhos relacionados

Os esquemas de proteção de *templates* biométricos propostos para mitigar os problemas de segurança e privacidade [19] [20] [21] [22] [23] [24] apresentam várias vulnerabilidades reportadas na literatura, [38] [39] [30] [31] [32]. Jain et al. classificam os esquemas de proteção de *template* biométrico em duas categorias principais [3]: 1) Esquemas baseados na transformação da característica; 2) Criptosistemas biométricos.

A ideia central por trás dos criptosistemas biométricos, também conhecidos como sistemas de ciframento biométrico, está em ou fundir a chave criptográfica com o *template* biométrico ou gerar uma chave criptográfica a partir do próprio *template* [49]. Logo, os criptosistemas biométricos podem ser classificados em duas categorias: 1) Esquemas de fusão de chave; 2) Esquemas de geração de chave.

Há os criptosistemas biométricos que usam dados auxiliares, ou seja, informações públicas sobre o *template* biométrico usadas na etapa de verificação. Embora os dados auxiliares em tese não vazem qualquer informação crítica sobre o *template* biométrico, Rathged et al. demonstraram que eles são vulneráveis a ataques de análise estatística dos dados [50]. Em outro trabalho, Ignatenko et al. mostraram como computar uma cota inferior na razão entre as taxas de sigilo e de vazamento de privacidade nos esquemas que fazem uso de dados auxiliares [51]. Adler apresenta em seu trabalho um ataque de *hill-climbing*

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

contra criptosistemas biométricos que informam o *score* da comparação [52], portanto esquemas de verificação não devem, na medida do possível, disponibilizar estes *scores*. Em [53], o ataque de *hill-climbing* é descrito para sistema e reconhecimento de íris. Em outro trabalho, Stoianov et. al. propuseram diversos ataques (impostores próximos, análise estatística de redundância do código corretor e ataques do tipo *non-randomness*) à criptosistemas biométricos [16].

Na literatura, *fuzzy commitment* [12] e esquemas de *fuzzy vault* [24] são categorizados sob esquemas de fusão e regeneração de chave. Esses esquemas visam combinar a chave criptográfica com o *template* biométrico. Em condições ideais, é inviável recuperar tanto o *template* biométrico quanto a chave sem conhecer os dados biométricos do indivíduo. Entretanto, esse não é o caso na prática porque a aleatoriedade do *template* biométrico não é uniformemente distribuída [30]. Combinado com o fato de os códigos corretores de erro usados em criptosistemas biométricos serem suscetíveis a ataques estatísticos, como ataques de histogramas ou decodificação presumida em modo *erasure* [16] [54], é possível a recuperação informação sobre o *template* mesmo sem conhecimento do dado biométrico.

Ignatenko et al. mostraram que esquemas de *fuzzy commitment* vazam informação sobre a chave criptográfica e, portanto, são suscetíveis a falhas de segurança e problemas com a privacidade dos dados biométricos [41] [43]. Zhou et al. também apresentam resultados argumentando que esquemas de *fuzzy commitment* vazam a privacidade dos dados biométricos [17] [18]. Chang et al. descrevem um ataque do tipo *non-randomness* contra um esquema de *fuzzy vault* que leva a distinção entre as minúcias e cristas em um template cifrado [55]. Kholmatov et al. realizaram um ataque de correlação contra esquemas de *fuzzy vaul*t [56].

Em esquemas de geração de chaves a partir de dados biométricos as chaves são geradas baseadas nos dados auxiliares e um dado *template* biométrico [3]. Esquemas de Extração de Chave Difusos são classificados como esquemas de geração de chaves a partir de dados biométricos que usam dados auxiliares [57] [58] [59] [60] [61]. Esses esquemas podem ser usados como um mecanismo de autenticação onde a verificação do indivíduo é feita utilizando seu próprio *template* biométrico como chave. Embora esquemas de extração de chave difusos possibilitem a geração de chaves criptográficas a partir de *templates* bio-

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

métricos, a estabilidade e a entropia das chaves geradas são dois grandes problemas desses esquemas [3]. Boyen et al. apontam diversas vulnerabilidades de esquemas de extração de chave difusos do ponto de vista de um atacante interno ou externo [62]. No ataque, eles demonstram que a construção inadequada de esboços difusos pode vazar informação sobre o segredo, assim como o uso de códigos enviesados podem deixar brechas para ataques de voto de maioria ou vazamento de informação no rotacionamento dos dados. Além disso, Li et al. mencionam que caso um adversário obtenha um esboço nesses esquemas, ele pode conseguir revelar a identidade do usuário [63].

As funções de *Biohashing* estão sendo muito estudadas nos últimos tempos [25] [26] [27] [28] [29]. Os esquemas baseados nessas funções são classificados como esquemas baseados em *salting*. É importante destacar que o *biohashing* é uma função completamente distinta do *hash* criptográfico. Embora as funções de *biohashing* tenham sido propostas para resolver aspectos relacionados à privacidade e à segurança, elas ainda apresentam problemas dessa natureza [33] [34] [35] [36]. Nesses artigos, os autores afirmam que o *biohash* pode ser revertido sob certas condições e um adversário pode estimar o *template* biométrico a partir do *biohash* do indivíduo. Consequentemente, quando *biohashes* são roubados da base de dados ou da memória de *smart cards*, estando em texto em claro, elas ameaçam a segurança do sistema como um todo, assim como a privacidade do indivíduo. O adversário malicioso pode, com isso, realizar ataques de personificação, se autenticando em lugar de outro indivíduo.

Esquemas baseados em transformações irreversíveis usam funções conhecidas como *one-way* para tornar o *template* biométrico seguro [64] [65] [66]. A chave secreta do indivíduo determina os parâmetros da função irreversível *one-way* e a chave só precisa ser apresentada no momento da verificação. Mesmo se o adversário obtiver a chave secreta ou o *template* biométrico transformado, ainda é computacionalmente inviável recuperar o *template* original. Por outro lado, esses esquemas sofrem do problema de compromisso entre distinguibilidade e irreversibilidade, o que afeta de forma significativa o desempenho de reconhecimento na prática.

Outra abordagem de segurança é o uso de primitivas de criptografia (por exemplo criptografia, *hashing*) para proteger *templates* biométricos. Estas obras geralmente focam em sistemas biométricos de impressão digital. Tuyls et al. propuseram o sistema de autenticação de impressão digital que incorpora *hashes* criptográficos [67]. Eles usam um

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

código corretor para obter *templates* biométricos exatos em cada sessão, similar ao que ocorrem com esquemas de extração de chave difusos. Eles armazenam os *hashes* criptográficos e os *templates* biométricos em banco de dados, realizando comparações no domínio do *hash*. Entretanto, não há garantia de se obter exatamente o mesmo *template* biométrico do indivíduo mesmo se o sistema possuir uma aplicação com código corretor real, já que é cotado ao limiar de capacidade de correção pré-estabelecido. Eles também usam dados auxiliares que são enviados por um canal público, o que representa uma falha de segurança. Ainda mais, o adversário pode ameaçar a segurança do sistema caso realize ataques contra o banco de dados, onde pode obter a identificação do indivíduo, os dados auxiliares e o hash desses dados. Embora o adversário não possa obter o dado biométrico em claro, ele pode obter todas as credenciais necessárias para ganhar acesso ao sistema.

Kerschbaum et al. propuseram um protocolo para comparar *templates* de impressões digitais sem realmente apresentá-los usando computação segura distribuída entre várias partes no modelo honesto-mas-curioso [68]. Na fase de inscrição, o usuário fornece seu *template* de impressão digital, pares de minúcias e PIN para o sistema. Assim, o verificador conhece os modelos de impressões digitais que são recolhidos na fase de inscrição. Embora o usuário não envie seus dados biométricos na autenticação, o verificador armazena os dados biométricos recolhidos do usuário e isso ameaça a sua privacidade no caso de um verificador malicioso. Além disso, um verificador malicioso pode usar as informações sobre as impressões digitais conhecidas para realizar uma autenticação maliciosa, ou seja, aplicar um ataque de personificação. Além disso, uma vez que a comparação de impressões digitais fornece os respectivos scores, ou as distâncias de Hamming entre elas, o adversário pode executar um ataque de *hill climbing* contra este sistema. Além destas falhas de segurança e privacidade, os autores se concentraram apenas na comparação de segurança entre os protocolos propostos, mas não apresentaram nenhuma solução segura para as abordagens maliciosas apontadas.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

3 RESULTADOS PARCIAIS

As questões importantes levantadas no projeto estão abordadas a seguir. As respostas aqui constantes ainda representam um posicionamento preliminar sobre os temas, baseado no que já foi pesquisado na literatura até o momento e nas premissas colocadas no projeto até então. Em geral, o posicionamento aqui apresentado reflete as opiniões do autor com base em seus conhecimentos e experiências anteriores sobre os temas correlatos, mas carece de melhor fundamento consolidado em base formal e revisão exaustiva da literatura, baseado em dados e análises de desempenho dos protocolos, o que se pretende alcançar com o futuro aprofundamento dos estudos.

Nenhuma análise feita até o momento é conclusiva, sendo esse apenas um resultado de um semestre de estudos. As recomendações feitas têm por base as primeiras revisões da literatura e os conhecimentos e experiências prévias do autor, correlatas ao tema. Todo estudo aqui apresentado ainda está em andamento, em fase preliminar. A finalidade desse relatório é apresentar os achados até o momento, demonstrando os rumos da pesquisa e o andamento e o nível de evolução do trabalho desenvolvido até o momento. Não é pretensão desse estudo, no atual estágio, a análise comparativa da performance dos sistemas, a análise comparativa da segurança dos protocolos apresentados na revisão da literatura, a análise comparativa do desempenho e da segurança das biometrias apontadas no projeto para emprego desses métodos, a pesquisa e análise minuciosa de produtos comerciais disponíveis no mercado ou o detalhamento de padrões e normas comerciais e ou governamentais

3.1 Biometrias adequadas

A primeira pergunta chave que visa ser respondida pelo projeto é sobre quais as biometrias adequadas à situação concreta em análise, ou seja, a identificação civil única no Brasil. Essa resposta depende de muitas variáveis e de um posicionamento estratégico. Porém, os estudos já realizados até o momento por outros grupos do projeto [69] já levantaram subsídios suficientes para se afirmar com ampla margem de segurança que as características biométricas mais adequadas à identificação civil no Brasil são a face, a impressão digital e a íris.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

A face e a impressão digital, na realidade, já são utilizadas há muito tempo pelo Estado brasileiro para a identificação civil, devendo, portanto, ser mantido esse legado, que já constitui base de informações históricas relevante. Embora sejam conhecidos problemas de duplicação de identidades e de registros falsos, ainda sim essa base contém importância na estrutura vigente, suficiente ao ponto de se manter e a sua preservação e compatibilidade. Além disso, a população já está habituada a fornecer esses dados biométricos para identificação, o que facilita na manutenção e na disseminação da cultura de coleta biométrica necessária ao sucesso da identificação civil.

Portanto, seria adicionado ao conjunto atualmente utilizado de características biométricas a coleta da íris de ambos os olhos [84]. A íris se mostrou a biometria mais promissora dentre as estudadas, e já está sendo utilizada em larguíssima escala para identificação civil internacionalmente, com destaque para a Índia. Esse fato tem contribuído para a redução significativa dos custos envolvidos na atividade de coleta e registro, com o surgimento de fabricantes diversos para atender a demanda por esse tipo de serviço. Além disso, a coleta da íris se resume a uma foto dos olhos, em definição de imagem e posicionamento de câmera especificamente estabelecidos, sendo as demais operações de âmbito computacional, como o processamento de imagem, a correção de erro, a criptografia do *template* e o armazenamento dos dados produzidos.

3.2 Comparação exata de *template* biométrico

Com a definição das características biométricas a serem utilizadas, outra questão de central importância que surge é sobre quais os algoritmos e protocolos de correção de erros a serem utilizados para permitir que a amostra biométrica produzida durante a autenticação ou a identificação do indivíduo possa ser comparada de modo exato ao *template* biométrico armazenado na base de dados biométricos central.

Esse tema foi abordado neste relatório. A revisão feita da literatura da área até agora parece indicar que a comparação exata de biometrias é ainda inviável, seja pela dificuldade de se corrigir os erros adicionados no processo de captura dos dados ou devido à natureza ruidosa da informação biométrica, seja pela baixa entropia resultante dos *templates* que passam por esse tipo de correção de erros, ou seja, pela baixa performance das

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

comparações quando realizadas sobre esse paradigma.

Portanto, considerados o atual nível de desenvolvimento dos algoritmos de correção de erros, o desempenho computacional exigido na prática por aplicações de identificação civil e os aspectos de segurança fundamentais envolvidos na geração e no armazenamento do *template,* recomenda-se um aprofundamento da pesquisa sobre proteção de *templates* biométricos, englobando outros métodos, como os métodos de criptografia homomórfica [48] [70].

3.3 Proteção e armazenamento seguro de *template* biométrico

Outro questionamento que surge naturalmente é quanto à proteção dos dados biométricos, já que as técnicas criptográficas usuais não são adequadas em aplicações com informação ruidosa, como é o caso da biometria.

Esse tema foi abordado no estudo realizado nesse relatório. A pesquisa sobre a proteção do *template* biométrico se mostrou extensa e complexa, pela grande quantidade de publicações na área sobre o tema e pela quantidade de aspectos de segurança envolvidos na tentativa de proteção desses dados, uma vez que são diversas as possibilidades de ataques e vazamentos de informação existentes.

A cifragem do *template* pode ser usada para a proteção do dado biométrico armazenado, seja em uma base de dados ou impresso em papel moeda. Com isso, proteger-se-ia a situação de vazamento de privacidade nos casos de acesso indevido à base de dados, a memória do cartão de identificação ou à imagem impressa em papel moeda. Porém, há diversas situações em que não se teria proteção, como no momento da comparação, da coleta de amostra e do tráfego dos dados pelo canal de comunicação.

É fundamental que um protocolo criptográfico com segurança demonstrável envolvendo todas as etapas da identificação, desde o registro inicial dos dados biométricos até a etapa de verificação, seja utilizado para se garantir a segurança do sistema como um todo. Há na literatura resultados nesse sentido, mas devido ao recente desenvolvimento dos resultados mais promissores, como é o caso de [48], não parece estar disponível comercialmente ainda uma solução com esse nível de robustez, já que se trata de pesquisa ainda em nível acadêmico.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Entretanto, se algumas premissas forem relaxadas, é possível obter armazenamento seguro e revogável do *template* biométrico no documento de identificação portado pelo cidadão, independente de qual seja. Mas isso terá impacto certo no tamanho do documento feito de papel, ou no custo do cartão com memória. Logo, para se estimar esses impactos, em termos de custos, desempenho dos sistemas, disponibilidade de soluções no mercado e restrições físicas dos dispositivos utilizados na verificação, precisa-se aprofundar a pesquisa sobre especificidades da implantação da proposta do projeto RIC.

Entrando em alguns detalhes, o armazenamento cifrado do *template* biométrico impresso em papel, em código de barras bidimensional, por exemplo, usando-se a técnica de *threshold homomorphic encryption* para garantir que futuramente o dado possa ser comparado sem a necessidade de decifrá-lo [71] [48] [70], que possa ser revogado caso seja vazado e que não permita a sua utilização para autenticação sem a obtenção de 2 chaves privadas distintas, a do cidadão e a do verificador. Essa é uma solução aparentemente adequada à situação delineada pelas premissas do projeto RIC, embora os resultados nessa direção na literatura da área ainda estejam em fase desenvolvimento acadêmico.

Já no caso do sistema como um todo, diversas técnicas criptográficas precisam ser combinadas para dar segurança adequada. A utilização de *biohash* parece ser atualmente a iniciativa mais adequada para a geração dos *templates,* conforme citado amplamente pela literatura apontada na revisão bibliográfica realizada neste relatório parcial. Além disso, precisa-se de um sistema de chaves públicas e privadas diferenciado, construído para funcionar de modo distinto do usual, apresentando um limiar para a combinação de chaves e operações em homomorfismo.

Em [8] são sugeridas como estratégias, para alcançar a revogabildade e a não-correlação dos dados auxiliares gerados pela biometria, o emprego de sistemas de proteção de *template* híbridos, com a combinação de criptosistemas com sistemas de transformação de parâmetros; ou o uso de métodos de autenticação com dois ou três fatores, com uso de dados auxiliares secretos, como um PIN ou uma senha.

Em [47] são citados alguns criptosistemas que utilizam mais de uma biometria e têm melhor performance comparada aos criptossitemas com uma única biometria.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

3.4 Premissas de segurança quanto a ataques, ameaças e vulnerabilidades

Uma decisão muito importante do projeto em relação à segurança é a definição do modelo de segurança, com as suas premissas e requisitos. Sabe-se que não é possível garantir segurança de 100% em sistema algum, fundamentalmente porque não há como se definir isso de modo que a disponibilidade ainda fosse requisito. É viável mitigar os principais e maiores riscos, ter sob controle as fragilidades conhecidas e gerenciar para minimizar danos e ter uma política de recuperação em casos de comprometimento da segurança e da privacidade das informações de um sistema. Esse é o paradigma atual de segurança da informação de qualquer sistema.

Assim, no caso do projeto RIC, uma demanda também colocada é a definição das premissas de segurança do processo de identificação civil como um todo. O que precisa ser seguro, o que se quer garantir ou o risco que se quer evitar precisam estar claros para se escolher os protocolos criptográficos adequados para a proteção do sistema como um todo. Não é possível cobrir todas as possíveis vulnerabilidades ou possibilidades de ataque com uma solução monolítica, fechada e de cunho genérico. A solução para o problema de segurança será formada por uma combinação cuidadosa e rigorosamente projetada para evitar ou impedir que vazamento de informações cruciais ou o comprometimento de partes vitais do sistema inviabilizem a prestação do serviço de identificação ou abram brechas para o cometimento de fraudes.

Além da não-correlação e da irreversibilidade, requisitos de segurança previsto na norma ISO/IEC 24745, a revogabilidade da biometria foi também uma premissa de segurança do projeto identificada após várias reuniões e discussões sobre o modelo de implantação com o grupo responsável pela gestão do projeto. Pode-se perceber que há uma grande preocupação em não vazar as informações sobre o dado biométrico, seja a partir da base de dados sob responsabilidade do Estado ou do documento de identificação sob responsabilidade do cidadão, e a possibilidade de se recuperar de um ataque que comprometa em definitivo o *template* gerado a partir da biometria do cidadão.

Destaca-se que a imagem da característica biométrica é extremamente difícil de se proteger, justamente por ser algo praticamente “público” que o indivíduo possui. Esse é o caso das três biometrias propostas para o projeto, ou seja, a face, a íris e a impressão digital. Então, a premissa deve ser realmente a proteção do *template* biométrico produzido a partir da imagem da característica biométrica. Para isso, o *template* precisa ser formado

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

da fusão de dois dados distintos, a biometria e uma chave. Essa chave deve ficar sob a posse do indivíduo, armazenada no cartão de identificação, por exemplo. Assim, o *template* não pode ser reconstituído sem as duas informações em conjunto. Mais do que isso, não pode ser utilizado sem a combinação das duas coisas. Ou seja, não adianta possuir a chave e não ter a biometria, ou vice-versa.

Há discussão, inclusive, sobre a utilização de autenticação baseada em três fatores, onde a posse de um *hardware* complementaria o esquema de segurança. Essa possibilidade é interessante e aparentemente incrementaria a segurança do sistema, caso seja implementada de modo correto. Para garantir isso, faz-se necessário estudo aprofundado sobre a forma correta de construção do protocolo usando essa combinação de fatores. Nesse relatório não há na revisão bibliográfia a abordagem desse tema. Desvantagens dessa abordagem seriam o provável custo do *hardware*, que em muitas situações se apresenta como proibitivo, a exemplo de soluções de segurança propostas por bancos comerciais, e a necessidade de o indivíduo ter que portar o *hardware,* dado o histórico de segunda via de documentos no Brasil.

A utilização da chave também possibilita a revogação do *template* em caso de comprometimento da privacidade. Soluções, como essa proposta, estão disponíveis na literatura da área e aparentemente também como produtos consolidados e disponíveis para venda no mercado.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

5 CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da SE/MJ e da UnB, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas. Destaca-se que nenhuma análise feita até o momento é conclusiva, sendo esse apenas um resultado de um semestre de estudos. As recomendações feitas têm por base as primeiras revisões da literatura e os conhecimentos e experiências prévias do autor, correlatas ao tema. Todo estudo aqui apresentado ainda está em andamento, em fase preliminar. A finalidade desse relatório é apresentar os achados até o momento, demonstrando os rumos da pesquisa e o andamento e o nível de evolução do trabalho desenvolvido até o momento. Não é pretensão desse estudo, no atual estágio, a análise comparativa da performance dos sistemas, a análise comparativa da segurança dos protocolos apresentados na revisão da literatura, a análise comparativa do desempenho e da segurança das biometrias apontadas no projeto para emprego desses métodos, a pesquisa e análise minuciosa de produtos comerciais disponíveis no mercado ou o detalhamento de padrões e normas comerciais e ou governamentais.

Os estudos já realizados até o momento por outros grupos do projeto [84] já levantaram subsídios suficientes para se afirmar com ampla margem de segurança que as características biométricas mais adequadas à identificação civil no Brasil são a face, a impressão digital e a íris. A face e a impressão digital, na realidade, já são utilizadas há muito tempo pelo Estado brasileiro para a identificação civil, devendo, portanto, ser mantido esse legado, que já constitui base de informações históricas relevante. Portanto, seria adicionado ao conjunto atualmente utilizado de características biométricas a coleta da íris de ambos os olhos.

Considerado o atual nível de desenvolvimento dos algoritmos de correção de erros, a performance exigida na prática por aplicações de identificação civil e os aspectos de segurança fundamentais envolvidos na geração e no armazenamento do *template*, nenhuma das técnicas de comparação exata de *templates* biométricos estudada pode ser recomendada ainda. Entretanto, recomenda-se o acompanhamento da pesquisa nessa área, inclusive de métodos com uso de multi-biometria que aparentemente fornecem um melhor desempenho.

Há também na literatura trabalhos com uso de criptografica homomórfica

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

promissores para a proteção do dado biométrico armazenado, seja em uma base de dados ou impresso em papel moeda. Mas devido à fase prematura dos protocolos e do evidente caráter acadêmico, não parece estar disponível comercialmente ainda uma solução com esse nível de robustez.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe do MJ, assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

REFERÊNCIAS

[1] A. K. Jain, A. Ross e S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. on Circuits and Systems for Video Technology*, pp. 4-20, 2004 vol. 4.

[2] S. Prabhakar, S. Pankanti e A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, pp. 33-42, 2003 vol.1.

[3] A. K. Jain, K. Nandakumar e A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, pp. 113:1-117:17, jan 2008.

[4] N. K. Ratha, J. H. Connell e R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, pp. 614-634, 2001 vol. 40.

[5] C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, pp. 14-25, 2007 vol. 26.

[6] T. A. M. Kevenaar, G. J. Schrijen, M. v. d. Veen, A. H. M. Akkermans e F. Zuo, "Face recognition with renewable and privacy preserving binary templates," em *IEEE Workshop on Automatic Identification Advanced Technologies*, 2005.

[7] X. Zhou, "PRIVACY AND SECURITY ASSESSMENT OF BIOMETRIC TEMPLATE PROTECTION," Technische Universität Darmstadt, 2011.

[8] K. Nandakumar, "Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice".*2015*.

[9] H. Feistel, "Cryptography and computer privacy," pp. 15-23, 1973.

[10] F. Hao, R. Anderson e J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput*, pp. 1081-1088, 2006.

[11] S. Kanade, D. Petrovska-Delacrtaz e B. Dorizzi, "Cancelable íris biometrics and using error correcting codes to reduce variability in biometric data," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 120-127, 2009.

[12] A. Juels e M. Wattenberg, "A fuzzy commitment scheme," *ACM Press*, pp. 28-36, 1999.

[13] G. I. Davida, Y. Frankel e B. J. Matt, "On enabling secure applications through off-line biometric identification," 1998.

[14] S. Tulyakov, F. Farooq e V. Govindaraju, "Symmetric hash functions for fingerprint minutiae," em *ICAPR* , 2005.

[15] Y. Sutcu, Q. Li e N. Memon, "How to protect biometric templates," em *SPIE Conf on Security, Steganography and Watermarking of Multimedia Contents IX*, 2007.

[16] A. S. A. e T. Kevenaar, "Security issues of biometric encryption," em *Science and Technology for Humanity (TIC-STH)*, , 2009.

[17] X. Zhou, "Privacy and security assessment of biometric template protection," *Information Technology*, 2012.

[18] X. Zhou, A. Kuijper, R. Veldhuis e C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," *Proceedings of the 2011 International Joint Conference on Biometrics*, pp. 1-8, 2011.

[19] J. Bringer, H. Chabanne, G. D. Cohen, B. Kindarji e G. Z´emor, "Optimal iris fuzzy sketches," *CoRR*, 2007.

[20] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti e A. Piva, "Privacy preserving fingercode authentication," *Proceedings of the 12th ACM workshop on Multimedia and security*, pp. 231-240, 2010.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

[21] K. Nandakumar, A. K. Jain e S. Pankanti, “Fingerprint-based fuzzy vault: Implementation and performance,” *IEEE Transactions on Information Forensics and Security*, pp. 744-757, 2007.

[22] Y. C. Feng, P. C. Yuen e A. K. Jain, “A hybrid approach for generating secure and discriminating face template,” *Trans. Info. For. Sec*, pp. 103-117, 2010.

[23] F. M. Bui, K. Martin, H. Lu, K. N. Plataniotis e D. Hatzinakos, “Fuzzy key binding strategies based on quantization index modulation (qim) for biometric encryption (be) applications,” *IEEE Transactions on Information Forensics and Security*, pp. 118-132, 2010.

[24] A. Juels e M. Sudan, “A fuzzy vault scheme,” *Des. Codes Cryptography*, pp. 237-257, 2006.

[25] C. Karabat e H. Erdogan, “A cancelable biometric hashing for secure biometric verification system,” *Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1082-1085, 2009.

[26] Z. Bai e D. Hatzinakos, “Lbp-based biometric hashing scheme for human authentication,” 2010.

[27] Y. W. Kuan, A. B. J. Teoh e D. C. L. Ngo, “Secure hashing of dynamic hand signatures using wavelet-fourier compression with biophasor mixing and 2n discretization,” *EURASIP J. Adv. Sig. Proc*, 2007.

[28] C. Rathgeb e A. Uhl, “Iris-biometric hash generation for biometric database indexing,” em *Pattern Recognition, International Conference on*, 2010.

[29] R. Lumini e L. Nanni, “An improved biohashing for human authentication,” *Pattern Recognition*, pp. 1057-1065, 2006.

[30] W. J. Scheirer e T. E. Boult, “Cracking fuzzy vaults and biometric encryption,” 2007.

[31] A. Adler, “Vulnerabilities in biometric encryption systems,” em *International Conference on Audio and Video based Biometric Person Authentication*, 2005.

[32] T. E. Boult, W. J. Scheirer e R. Woodworth, “Revocable fingerprint biotokens: Accuracy and security analysis,” em *CVPR*, 2007.

[33] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel e J. You, “An analysis of biohashing and its variants,” em *Pattern Recognititon*, 2006.

[34] K. Kommel e C. Vielhauer, “Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting,” em *Proceedings of the 12th ACM workshop on Multimedia and security*, 2010.

[35] K. H. Cheung, A. W.-K. Kong, J. You e D. Zhang, “An analysis on invertibility of cancelable biometrics based on biohashing,” em *CISST*, 2005.

[36] K. Kummel, C. Vielhauer, T. Scheidat, D. Franke e J. Dittmann, “Handwriting biometric hash attack: a genetic algorithm with user interaction for raw data reconstruction,” em *Proceedings of the 11th IFIP TC 6/TC 11 international conference on Communications and Multimedia Security*, 2010.

[37] S. Cimato, M. Gamassi, V. Piuri, R. Sassi e F. Scotti, “A biometric verification system addressing privacy concerns,” em *CIS*, 2007.

[38] T. Matsumoto, H. Matsumoto, K. Yamada e S. Hoshino, “Impact of artificial ”gummy” fingers on fingerprint systems,” em *Datenschutz und Datensicherheit*, 2002.

[39] T. v. d. Putte e J. Keuning, “Biometrical fingerprint recognition: Don’t get your fingers burned,” em *CARDIS*, 2000.

[40] K. Simoens, P. Tuyls e B. Preneel, “Privacy weaknesses in biometric sketches,” em *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, 2009.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

[41] T. I. a. F. M. J. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Transactions on Information Forensics and Security,* pp. 337-348, 2010.

[42] K. Simoens, J. Bringer, H. Chabanne e S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Transactions on Information Forensics and Security,* pp. 833-841, 2012.

[43] T. Ignatenko e F. M. J. Willems, "Biometric systems: privacy and secrecy aspects," *IEEE Transactions on Information Forensics and Security,* pp. 956-973, 2009.

[44] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk e T. Toft, "Privacy-preserving face recognition," *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies,* pp. 235-253, 2009.

[45] A.-R. Sadeghi, T. Schneider e I. Wehrenberg, "Efficient privacy preserving face recognition," *ICISC,* pp. 229-244, 2009.

[46] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva e F. Scotti, "A privacy compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," *Biometrics: Theory Applications and Systems (BTAS),* 2010.

[47] C. Rathgeb e A. Uhl, "Survey on Biometric Cryptosystems and cancelable biometrics," *Eurasip Journals,* 2011.

[48] C. Karabat, M. S. Kiraz, H. Erdogan e E. Savas, "THRIVE: Threshold Homomorphic encryption based secure and privacy preserving bIometric VErification system," [Online]. Available: http://arxiv.org/abs/1409.8212. [Acesso em set 21 2014].

[49] S. P. U. Uludag, S. Pankanti e A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE,* pp. 948-960, 2004.

[50] C. Rathgeb e A. Uhl, "Statistical attack against iris-biometric fuzzy commitment schemes," *biometric fuzzy commitment schemes," in* , pp. 23-30, 2011.

[51] T. Ignatenko e F. Willems, "Secret rate - privacy leakage in biometric systems," *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory,* pp. 2251-2255, 2009.

[52] A. Adler, "Vulnerabilities in biometric encryption systems," *International Conference on Audio and Video based Biometric Person Authentication,* pp. 1100-1109, 2005.

[53] C. Rahtgeb e A. Uhl, "Attacking iris recognition: An efficient hillclimbing technique," *Proc. ICPR,* 2010.

[54] A. Stoianov, "Security of error correcting code for biometric encryption," *Eighth Annual Conference on Privacy, Security and Trust,* 2010.

[55] E.-C. Chang, R. Shen e F. W. Teo, "Finding the original point set hidden among chaff," *Proceedings of the 2006 ACM Symposium on Information,* pp. 182-188, 2006.

[56] A. K. a. B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," 2008.

[57] Y. Dodis, R. Ostrovsky, L. Reyzin e A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput,* 2008.

[58] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin e A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," *IEEE Transactions on Information Theory,* pp. 6207-6222, 2012.

[59] Y. Sutcu, L. Qiming e N. Memon, "Design and analysis of fuzzy extractors for faces,"

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

Proceedings of SPIE Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification , 2009.

[60] T. S. O. a. A. B. J. Teoh, "Fuzzy key extraction from fingerprint biometrics based on dynamic quantization mechanism," *Proceedings of the Third International Symposium on Information Assurance and Security,* pp. 71-76, 2007.

[61] A. Arakala, J. Jeffers e K. J. Horadam, "Fuzzy extractors for minutiae-based fingerprint authentication," *ICB'07,* pp. 760-769, 2007.

[62] X. Boyen, "Reusable cryptographic fuzzy extractors," *Proceedings of the 11th ACM conference on Computer and communications security,* pp. 82-91, 2004.

[63] M. G. Q. L. a. E.-C. Chang, "Fuzzy extractors for asymmetric biometric representation," *Proceedings of IEEE Workshop on Biometrics,* 2008.

[64] Y. Sutcu, H. T. Sencar e N. Memon, "A secure biometric authentication scheme based on robust hashing," *Proceedings of the 7th workshop on Multimedia and security,* pp. 111-116, 2005.

[65] A. T. B. Jin, K.-A. Toh e W. K. Yip, "2^N discretisation of biophasor in cancellable biometrics," *ICB,* pp. 435-444, 2007.

[66] B. Yang, C. Busch, P. Bours e D. Gafurov, "Robust minutiae hash for fingerprint template protection," *Media Forensics and Security,* 2010.

[67] Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen e R. N. J. Veldhuis, "Practical biometric authentication with template protection," *AVBPA,* pp. 436-446, 2005.

[68] F. Kerschbaum, M. J. Atallah, D. M'Raïhi e J. R. Rice, "Private fingerprint verification without local storage," *ICBA,* pp. 387-394, 2004.

[69] F. M. Buiati, P. A. O. d. Paula e W. R. d. Fonseca, "Relatório de Biometria Projeto RIC," UnB, 2014.

[70] G. Penn, G. Pötzelsberger, M. Rohde e A. Uhl, "Customisation of Paillier homomorphic encryption for efficient binary biometric feature vector matching," *Biometrics Special Interest Group (BIOSIG),* , pp. 1-6, 2014.

[71] R. Cramer, I. Damgard e J. B. Nielsen, "Multiparty computation from threshold homomorphic encryption," *EUROCRYPT,* pp. 280-299, 2001.

INCOMPLETO

Confidencial.
Este documento foi elaborado pela Universidade de Brasília (UnB) para a MJ/SE.
É vedada a cópia e a distribuição deste documento ou de suas partes sem o consentimento, por escrito, da MJ/SE.

INCOMPLETO

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br