Autenticação do Código de Iris Usando Busca por Rotação e Voto de Maioria

G. N. Melo, V. C. da Rocha Jr. e J. S. Lemos-Neto

***Resumo*— Sabe-se que o desempenho de sistemas biométricos para identificação de usuário baseados em código de íris melhora quando se consegue reduzir a distância de Hamming entre o código de íris de referência e o código de íris de teste empregados. O objetivo deste artigo é propor e analisar, por meio de simulação em computador, a técnica de decisão por voto de maioria aplicada à identificação biométrica por meio do código de íris. Os resultados obtidos indicam que a distância de Hamming média é reduzida em todas as bases de dados testadas. O melhor resultado obtido foi uma redução de 19,79% para a distância de Hamming média. Para a base de dados NIST-ICE(exp1) foi obtida um redução de 68,4% para a taxa de falsa rejeição (FRR - *false rejection rate*), em comparação com resultados publicados anteriormente.**

***Palavras-Chave*— voto de maioria, iris, biometria, identificação, código.**

***Abstract*— It is well known that the performance of biometric systems for user identification based on the iris code improves when a reduction in the Hamming distance between the iris reference code and the iris test code employed is achieved. The main aim in this paper is to propose and analyze by means of computer simulation the technique of majority voting applied to biometric identification employing the iris code. The results obtained indicate a reduction on average Hamming distance in all data bases tested. The highest reduction on average Hamming distance was 19.79%. For the NIST-ICE(exp1) data base a reduction in false rejection ratio of 68.4% was obtained, in comparison to a previously published result.**

***Keywords*— majority voting, iris, biometrics, identification, coding.**

I. Introdução

De acordo com [1], a utilização da biometria tem crescido significativamente nos últimos anos, o que aumenta a preocupação sobre a privacidade individual e o sigilo dos dados, pois as soluções biométricas convencionais exigem o armazenamento direto dos dados pessoais do usuário [2, p. 19-20]. Por outro lado, a criptografia de chave secreta é capaz de assegurar alta privacidade aos dados desde que a chave criptográfica seja mantida em segredo e, além disso, seja tão longa e aleatória quanto possível para proporcionar o nível de segurança necessário. Assim, um modo de garantir a privacidade e a autenticidade dos dados é combinar criptografia e biometria, haja vista a natureza complementar dessas duas ferramentas de segurança. Um dos problemas desta combinação é lidar com a precisão exigida pelos sistemas criptográficos e a variabilidade inerente dos dados biométricos. Uma das abordagens utilizadas para obter chaves criptográficas a partir de dados biométricos, conhecida como *regeneração de chave criptográfica*, lida com essa necessidade empregando códigos corretores de erro [3].

Trabalhos recentes na área de biometria têm focado, principalmente, em novos métodos para obter códigos de íris [4]–[6]. Não obstante, aspectos de segurança de sistemas biométricos também têm sido alvos de interesse de trabalhos recentes [7]–[9]. Neste artigo, o foco é no desempenho de sistemas biométricos de regeneração de chave criptográfica que, relativamente, têm recebido pouca atenção nos últimos anos [1], [10].

Sabe-se que o desempenho de sistemas biométricos para identificação de usuário baseados em código de íris melhora quando se consegue reduzir a distância de Hamming entre o código de íris de referência e o código de íris de teste empregados. O objetivo deste artigo é propor e analisar, por meio de simulação em computador, a técnica de decisão por voto de maioria aplicada à identificação biométrica por meio do código de íris. Os resultados obtidos indicam que a distância de Hamming média é reduzida em todas as bases de dados testadas. O melhor resultado obtido foi uma redução de $19,79\%$ para a distância de Hamming média. Para a base de dados NIST-ICE(exp1) foi obtida um redução de $68,4\%$ para a taxa de falsa rejeição, em comparação com resultados publicados anteriormente.

O restante deste artigo está assim organizado. A Seção II aborda a técnica de decisão por voto de maioria, a Seção III descreve o sistema biométrico empregado para regeneração de chave criptográfica, o qual depende fundamentalmente da identificação do código de íris. A Seção IV apresenta simulação e resultados obtidos e o artigo é encerrado na Seção V, a qual apresenta as principais conclusões e sugestões.

II. Técnica de voto de maioria

A técnica de voto de maioria é bastante conhecida no contexto de códigos corretores de erros [3, p. 273]. Neste artigo, a técnica de voto de maioria consiste em analisar duas ou mais sequências, comparando-as coordenada a coordenada, e produzindo como resultado a sequência denominada de *sequência majoritária*, na qual o valor binário de cada coordenada corresponde ao valor do voto de maioria calculado naquela coordenada dentre as sequências examinadas. Em outras palavras, observa-se o valor de uma determinada coordenada em todas as sequências consideradas e realiza-se o voto de maioria, contando a quantidade de 0's e de 1's, no caso de sequências binárias, e atribui-se como valor final aquele que for a maioria na contagem realizada.

Para exemplificar a técnica de voto de maioria, considere três sequências binárias de comprimento $n = 8$ cada uma,

O endereço dos autores é Grupo de Pesquisa em Comunicações, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, 50740-550, Recife, PE, E-mails: {guilherme.nmelo, vcr, jose.lemosnt}@ufpe.br.

$\mathbf{x} = (0,1,0,1,1,0,1,0)$, $\mathbf{y} = (0,1,0,0,0,0,1,0)$ e $\mathbf{z} = (0,1,0,1,0,1,1,1)$. A sequência majoritária $\mathbf{m}$ é obtida aplicando a técnica de voto de maioria às sequências $\mathbf{x}$, $\mathbf{y}$ e $\mathbf{z}$ da seguinte forma. Cada coordenada m_i de $\mathbf{m}$ é obtida pelo voto de maioria das respectivas coordenadas x_i, y_i e z_i, em que $0 \leq i \leq 7$. Para $i = 3$, obtém-se $m_3 = 1$, pois $x_3 = 1$, $y_3 = 0$ e $z_3 = 1$. Assim procedendo para os demais valores de i resulta $\mathbf{m} = (0,1,0,1,0,0,1,0)$.

Na primeira coluna da Tabela I são exibidas as sequências $\mathbf{x}$, $\mathbf{y}$ e $\mathbf{z}$, aqui consideradas como sequências de referência, a sequência majoritária $\mathbf{m}$ e a sequência de teste $\mathbf{s}$. A Tabela I apresenta valores da distância de Hamming (HD) entre pares de sequências. Analisando os valores de HD verifica-se que $d(\mathbf{m},\mathbf{s})$ entre as sequências $\mathbf{m}$ e $\mathbf{s}$ é igual a 1. Comparando $d(\mathbf{m},\mathbf{s})$ com $d(\mathbf{x},\mathbf{s}) = 2$, $d(\mathbf{y},\mathbf{s}) = 2$ e $d(\mathbf{z},\mathbf{s}) = 1$, percebe-se que usar $\mathbf{m}$ como sequência de referência reduz o valor de $d(\mathbf{m},\mathbf{s})$.

TABELA I

EXEMPLO DO CÁLCULO DA HD USANDO VOTO DE MAIORIA.

Sequência	$\mathbf{x}$ (HD)	$\mathbf{y}$ (HD)	$\mathbf{z}$ (HD)	$\mathbf{s}$ (HD)	$\mathbf{m}$ (HD)
$\mathbf{x}$ = 01011010	00000000 (0)	00011000 (2)	00001101 (3)	00001100 (2)	00001000 (1)
$\mathbf{y}$ = 01000010	00011000 (2)	00000000 (0)	00010101 (3)	00010100 (2)	00010000 (1)
$\mathbf{z}$ = 01010111	00001101 (3)	00010101 (3)	00000000 (0)	00000001 (1)	00000101 (2)
$\mathbf{s}$ = 01010110	00001100 (2)	00010100 (2)	00000001 (1)	00000000 (0)	00001000 (1)
$\mathbf{m}$ = 01010010	00001000 (1)	00010000 (1)	00000101 (2)	00000100 (1)	00000000 (0)

O exemplo discutido com o auxílio da Tabela I indica que utilizar a técnica de voto de maioria para obter uma sequência de referência parece promissora. Assim, na sequência, utilizam-se as bases de dados BIOSECURE [11], CASIA [11] e NIST-ICE [12], que possuem códigos de íris de teste e códigos de íris de referência, com o objetivo de gerar códigos de íris de referência por meio da técnica de voto de maioria e avaliar o impacto desta técnica no cálculo da HD.

III. SISTEMA BIOMÉTRICO DE REGENERAÇÃO DE CHAVE CRIPTOGRÁFICA

Exibe-se na Figura 1, por meio de um diagrama de blocos, o sistema biométrico de regeneração de chave criptográfica empregando a técnica de voto de maioria. O sistema proposto é semelhante ao apresentado em [10], com o acréscimo do bloco de pré-processamento denotado por "Manipulação do código de íris por decisão majoritária". Nesse bloco, aplica-se a técnica de voto de maioria, discutida na Seção II, para gerar o código de íris de referência, denotado por θ_{ref}. Desse ponto em diante, o funcionamento do sistema da Figura 1 é similar ao do sistema proposto em [10]. Por fim, vale ressaltar que os códigos de íris de teste, usados na fase de verificação do usuário, são denotados por θ_{sam}.

A. Pré-processamento usando voto de maioria

Em [10], as bases de dados BIOSECURE e CASIA são denominadas *regulares*, pois possuem a mesma quantidade de códigos de íris de referência e de códigos de íris de teste para cada usuário. No total são 10 códigos de íris de referência por usuário, de modo que se podem escolher até $i = 9$ códigos de íris para gerar θ_{ref}.

Ainda segundo [10], a base de dados do NIST-ICE é denominada *irregular*. Nesse caso, a quantidade de códigos

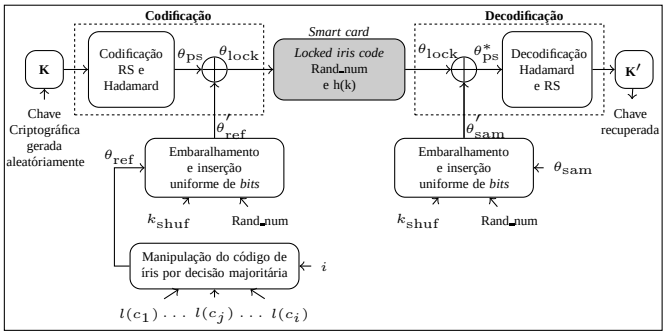

Fig. 1. Sistema biométrico de recuperação de chave criptográfica utilizando a técnica de voto de maioria como pré-processamento. Os códigos de íris das bases de dados, que são usados como referência, são aplicados ao bloco de pré-processamento.

de íris para cada usuário não é a mesma, variando entre 1 e 31 códigos. Na base de dados NIST-ICE não há uma distinção entre os códigos de íris que são usados como referência e os que são usados como teste. Para o teste de usuário genuíno, a escolha é realizada da seguinte maneira. O código de íris θ_1, para o usuário U, é escolhido como referência e compara-se θ_1 com os demais códigos de íris do usuário U, que nesse ponto são usados como códigos de íris de teste. Depois de realizadas todas as comparações possíveis para θ_1, o código de íris θ_2 é escolhido como código de referência, sendo comparado com os demais códigos restantes, assim como foi feito para θ_1. Esse processo continua até que todos os códigos de íris do usuário U tenham sido usados como códigos de referência.

IV. SIMULAÇÃO E RESULTADOS

Nesta seção apresentam-se os métodos usados para realizar as simulações e os resultados obtidos para o desempenho do sistema da Figura 1. Todas as simulações foram realizadas em C++ num computador equipado com processador Intel core i7 de terceira geração, disco rígido SSD com 128GB e 8GB de memória RAM.

A. Simulação

Os testes com todas as bases de dados foram realizados com os mesmos valores de i para grupos contendo i códigos de íris distintos, ou seja, $i = \{3,5,7,9\}$. Porém, foi necessário, em alguns casos, limitar o valor de i na base de dados NIST-ICE, por conta da quantidade máxima de códigos de íris disponíveis nessa base de dados.

Para as bases de dados regulares foram feitos experimentos com todas as possíveis combinações de códigos para cada i. Na Tabela IV, está indicado para cada i a quantidade total de testes, assim como a combinação de códigos de íris que resultou na menor HD, e a combinação de códigos que resultou na maior HD.

Para as bases de dados BIOSECURE e CASIA, considerando a quantidade de códigos de íris usados para gerar θ_{ref}, foram realizadas simulações com todas as possíveis combinações. Para $i = 3$ são possíveis 120 combinações, i.e., C_{10}^3 combinações. Nesse caso foram realizadas duas rodadas de 120 experimentos, totalizando 240 experimentos. Para $i = 5$ resulta $C_{10}^5 = 252$ e foram realizados 252 experimentos. Para $i = 7$ resulta $C_{10}^7 = 120$ e foram realizados 240

experimentos (duas rodadas de 120). Para $i = 9$ resulta $C_{10}^{9} = 10$ e foram realizados 240 experimentos (vinte e quatro rodadas de 10 experimentos cada). Desse modo, a quantidade de experimentos manteve-se em 240 para $i = 3$, $i = 7$ e $i = 9$, enquanto que para $i = 5$ foram realizados 252 experimentos. O total de experimentos realizados para cada base de dados foi de 972. O tempo médio de cada experimento foi, aproximadamente, 31 minutos e o tempo total, para ambas as bases de dados foi de, aproximadamente, 41 dias, 22 horas e 33 minutos. O objetivo foi manter o mais uniforme possível a quantidade de experimentos para os diferentes valores de i. Os resultados percentuais para FRR, apresentados nas Tabelas VI e VII na sequência deste artigo, são as médias obtidas a partir de todas as rodadas de experimentos realizadas.

Para a base de dados NIST-ICE, a quantidade máxima M de códigos de íris disponíveis para um determinado usuário é variável, e não existe separação entre códigos de referência e códigos de teste. O *software* utilizado é programado para identificar o número mais adequado de códigos de íris e, se necessário, reduzir automaticamente para o maior valor possível de i em cada teste específico. Por exemplo, se para um determinado usuário $M = 7$, então o *software* utiliza, no máximo, $i = 5$, pois não há, na base de dados, códigos de íris de teste específicos e, portanto, pelo menos um dos 7, deve ser usado como θ_{sam}. Como restam 6 códigos de íris para aplicar o voto de maioria e a quantidade par pode resultar em empate, opta-se por usar 5 códigos de íris.

A implementação também verifica quanto à "contaminação" de códigos de íris de referência em relação ao código de íris de teste, não permitindo que o código de íris de teste faça parte da composição dos códigos de íris de referência usados na decisão por voto de maioria. A escolha dos códigos de referência, para a base de dados do NIST-ICE, é então feita numa lista $\mathcal{L}$ de códigos numerados de 1 a M. A regra adotada neste trabalho para a escolha de até nove códigos é descrita a seguir.

Para um dado valor de i fixado, é necessário selecionar i códigos de íris c_j, $1 \leq j \leq i$, cuja posição $l(c_j)$, $1 \leq l(c_j) \leq M$, na lista $\mathcal{L}$ é indicada na Tabela II, na qual $1 \leq i \leq 9$. Após a escolha dos i códigos c_j, que são usados para gerar θ_{ref}, cada c_j é comparado com todas as escolhas anteriores e com θ_{sam}. Caso o c_j atual já tenha sido escolhido entre os códigos c_j anteriores, o código que representa o c_j atual é substituído pelo código na lista $\mathcal{L}$ associado à posição $(l(c_j) \mod M) + 1$, que passa a compor o novo código de íris de referência θ_{ref}. Desse modo, garante-se que $j = j_1 \neq j_2$, o que implica em $c_{j_1} \neq c_{j_2}$ e em $c_j \neq \theta_{\mathrm{sam}}$, $1 \leq j \leq M$.

Cada uma das oito linhas na Tabela III, constituem exemplos de escolha dos códigos de íris de referência para compor θ_{ref}. A partir da terceira coluna, os números indicados na Tabela III são as posições de cada código na lista $\mathcal{L}$ correspondente, tanto para os códigos de referência quanto para os códigos de teste. Por exemplo, na terceira linha, $l(c_5) = 13$ significa que c_5 ocupa a décima terceira posição na lista $\mathcal{L}$ na base de dados, e é escolhido como um dos códigos de íris, que irão compor o código de referência. Essa posição, pela fórmula usada para a localização a priori de c_5 seria a 12, porém a posição 12 já é usada para o código de teste, por isso faz-se c_5 assumir o código na posição $(l(c_5) \mod 15) + 1$, na lista $\mathcal{L}$, i.e., a posição de número 13. Para este exemplo, o código de íris de referência θ_{ref}, que será usado no teste, será composto por: $l(c_1)$, $l(c_2)$, $l(c_3)$, $l(c_4)$ e $l(c_5)$, ou seja, pelas posições, respectivamente: 11, 8, 15, 4 e 13.

TABELA II

LISTA PARA ESCOLHA A PRIORI DA BASE DE DADOS NIST-CIE, DOS CÓDIGOS DE REFERÊNCIA A SEREM USADOS PARA GERAR θ_{ref}.

Número de ordem	Código	Posição na lista $\mathcal{L}$
primeiro	c_1	$l(c_1) = 1$
segundo	c_2	$l(c_2) = \lceil M/2 \rceil$
terceiro	c_3	$l(c_3) = M$
quarto	c_4	$l(c_4) = \lceil M/4 \rceil$
quinto	c_5	$l(c_5) = \lceil 3M/4 \rceil$
sexto	c_6	$l(c_6) = \lceil 3M/8 \rceil$
sétimo	c_7	$l(c_7) = \lceil 5M/8 \rceil$
oitavo	c_8	$l(c_8) = \lceil M/8 \rceil$
nono	c_9	$l(c_9) = \lceil 7M/8 \rceil$

B. Resultados

Na Tabela IV, pode-se observar o que ocorre com os valores máximo, mínimo e médio para a HD quando é aplicada a técnica de voto de maioria a grupos contendo i códigos de íris, $i = \{3, 5, 7, 9\}$. É possível observar que quanto maior o valor de i, menor é o valor da HD média. Ainda na Tabela IV, observa-se que a redução percentual da HD média quando $i = 9$, com relação a $i = 1$ (i.e., sem aplicação da técnica de voto de maioria), é de $12,73\%$, $6,77\%$, $19,79\%$ e $18,99\%$, para as bases de dados BIOSECURE, CASIA, NIST-ICE(exp1) e NIST-ICE(exp2), respectivamente. Esse ganho percentual indica que ao usar um código de íris de referência obtido por meio da técnica de voto de maioria com $i = 9$, há uma redução da FRR, pois a distância de Hamming média entre θ_{ref} e θ_{sam} é reduzida.

TABELA IV

DISTÂNCIA DE HAMMING PARA USUÁRIOS GENUÍNOS NAS BASES DE DADOS BIOSECURE, CASIA E NIST-ICE, COM $i \in \{1, 3, 5, 7, 9\}$ CÓDIGOS DE ÍRIS. (OBS.: N/D - NÃO DISPONÍVEL).

	Base de Dados		BIOSECURE	CASIA	NIST-ICE (exp1)	NIST-ICE (exp2)
1 código	Numeração dos códigos combinados	Melhor	1	1	N/D	N/D
		Pior	1	1	N/D	N/D
		Total de testes	1	1	N/D	N/D
	Distância de Hamming	Min	54	155	114	123
		Max	617	645	641	636
		Média	289,99	378,65	340,07	346,56
3 códigos	Numeração dos códigos combinados	Melhor	(5,8,9)	(4,9,10)	N/D	N/D
		Pior	(2,3,4)	(2,3,4)	N/D	N/D
		Total de testes	120	120	N/D	N/D
	Distância de Hamming	Min	55	122	118	137
		Max	602	647	603	598
		Média	267,51	362,77	297,62	304,67
5 códigos	Numeração dos códigos combinados	Melhor	(2,5,8,9,10)	(1,2,4,6,8)	N/D	N/D
		Pior	(1,3,4,5,8)	(2,4,5,6,9)	N/D	N/D
		Total de testes	252	252	N/D	N/D
	Distância de Hamming	Min	52	119	112	133
		Max	599	645	581	594
		Média	259,55	357,25	285,29	291,05
7 códigos	Numeração dos códigos combinados	Melhor	(2,5,6,7,8,9,10)	(1,2,4,6,7,8,10)	N/D	N/D
		Pior	(1,2,3,4,5,7,10)	(2,3,4,5,6,8,9)	N/D	N/D
		Total de testes	120	120	N/D	N/D
	Distância de Hamming	Min	61	133	116	135
		Max	590	641	565	608
		Média	255,48	354,52	278,08	285,89
9 códigos	Numeração dos códigos combinados	Melhor	(1,2,4,5,6,7,8,9,10)	(1,2,3,4,5,6,7,8,10)	N/D	N/D
		Pior	(1,2,3,4,5,7,8,9,10)	(2,3,4,5,6,7,8,9,10)	N/D	N/D
		Total de testes	10	10	N/D	N/D
	Distância de Hamming	Min	70	139	116	129
		Max	576	633	581	596
		Média	253,09	353,03	272,78	280,74
Redução da HD (1 cód x 9 cód)			12,73%	6,77%	**19,79%**	18,99%

Todos os testes realizados foram executados com a busca por rotação [10] ativada. Na Tabela V, pode-se observar o

TABELA III

EXEMPLO DE ESCOLHA DOS CÓDIGOS USADOS NOS TESTES DA BASE DE DADOS NIST-ICE. (*) INDICA QUE É NECESSÁRIO PELO MENOS UMA REDUÇÃO MÓDULO M DO ÍNDICE LOCALIZADOR NA LISTA $\mathcal{L}$.

M	i	θ_{sam}	θ_{ref}	$l(c_1) = 1$ $c_1 = \theta_{\mathrm{ref}}$	$l(c_2) = \lceil$M/2$\rceil$	$l(c_3) = M$	$l(c_4) = \lceil$M/4$\rceil$	$l(c_5) = \lceil$3M/4$\rceil$	$l(c_6) = \lceil$3M/8$\rceil$	$l(c_7) = \lceil$5M/8$\rceil$	$l(c_8) = \lceil$M/8$\rceil$	$l(c_9) = \lceil$7M/8$\rceil$
7	3	5	6	6	4	7	-	-	-	-	-	-
7	9	3	1	1	4	7	2	6	-	-	-	-
15	5	12	11	11	8	15	4	13*	-	-	-	-
15	7	15	3	3	8	1*	4	12	6	10	-	-
25	9	1	7	7	13	25	8*	19	10	16	4	22
25	3	3	19	19	13	25	-	-	-	-	-	-
31	7	6	25	25	16	31	8	24	12	20	-	-
31	9	27	2	2	16	31	8	24	12	20	4	28

valor médio da FRR(%), obtido para $1 \leq t_{\mathrm{RS}} \leq 10$, em que t_{RS} é a capacidade de correção de erros do código Reed-Solomon [3, p. 81]. Ainda na Tabela V, observa-se que para $1 \leq t_{\mathrm{RS}} \leq 10$, os piores resultados obtidos com $i = 9$ são melhores que os resultados obtidos com $i = 1$. Assim, pode-se utilizar qualquer combinação aleatória permitida de i códigos de iris, $i \neq 1$, para tomar a decisão por voto de maioria, que o resultado obtido será melhor do que no caso em que $i = 1$.

TABELA V

VALOR MÉDIO DA FRR(%) USANDO 1 CÓDIGO E VOTO DE MAIORIA COM 9 CÓDIGOS (240 EXPERIMENTOS) PARA A BASE DE DADOS BIOSECURE.

t_{RS}	1 código	9 códigos			
		média	mínimo	máximo	desvio padrão
1	**15,1500**	**10,3804**	9,4833	11,2667	0,3075
2	**11,0400**	**8,3610**	7,7667	8,9000	0,2362
3	**8,6300**	**7,3429**	6,8167	7,8167	0,1727
4	**7,4900**	**6,7167**	6,2833	7,1333	0,1533
5	**6,6300**	**6,1051**	5,6167	6,5500	0,1793
6	**5,9900**	**5,4638**	4,9167	5,9167	0,2268
7	**5,3900**	**4,7697**	3,9667	5,3833	0,2553
8	**4,7400**	**4,0755**	3,4667	4,6500	0,2137
9	**4,0600**	**3,4415**	2,8833	3,8500	0,1842
10	**3,4000**	**2,7778**	2,2000	3,2833	0,1949

Os resultados obtidos para a base de dados BIOSECURE usando uma única íris estão na Tabela VI. Na coluna em que $i = 1$, estão os resultados obtidos em [10] que podem ser comparados com os resultados das colunas em que $i \in \{3, 5, 7, 9\}$. É possível observar na Tabela VI que os valores percentuais da FRR, na maioria dos casos, tendem a diminuir quanto maior for o valor do i, considerando o mesmo valor de t_{RS}. Para comparar o método usado em [10] com o método proposto neste artigo, são analisados os percentuais de erro em função de t_{RS} na Tabela VI. Para $t_{\mathrm{RS}} = 1$, resulta FRR = 15,15% quando $i = 1$, e resulta FRR = 10,38% quando $i = 9$, o que representa uma redução de 4,77% na FRR. Para a base de dados BIOSECURE, o melhor resultado é obtido para $i = 9$.

Na Tabela VII, estão os resultados obtidos utilizando uma única íris, para a base de dados CASIA. Para $t_{\mathrm{RS}} = 1$, resulta FRR = 23,11% quando $i = 1$, e resulta FRR = 12,38% quando $i = 9$, o que representa uma redução de 10,73% na FRR.

Para a base de dados NIST-ICE, devido à variação da quantidade de códigos de íris por usuário, não é possível fazer experimentos com todas as combinações possíveis. Porém, o método escolhido para utilização dos códigos de referência permite testar diversas combinações diferentes. Na Tabela VIII estão os resultados para uma única íris, obtidos com a base de dados NIST-ICE. Para $t_{\mathrm{RS}} = 1$, $i = 1$ e uma íris para o olho direito (exp1), obtém-se FRR = 21,37% e para $i = 9$ obtém-se FRR = 6,76%, que representa uma redução de 14,61% na

TABELA VI

FRR(%) PARA A BASE DE DADOS BIOSECURE EMPREGANDO BUSCA POR ROTAÇÃO COM $i \in \{1, 3, 5, 7, 9\}$. (OBS.: N/D - NÃO DISPONÍVEL).

$C_{10}^{i} \rightarrow$	1	120	252	120	10
Rodadas $\rightarrow$	N/D	2	1	2	24
Total $\rightarrow$	N/D	240	252	240	240
$t_{\mathrm{RS}} \downarrow$	1 cód	3 cód	5 cód	7 cód	9 cód
1	**15,1500**	11,4974	10,7935	10,5343	**10,3804**
2	**11,0400**	8,7883	8,5284	8,4058	**8,3610**
3	**8,6300**	7,5006	7,4091	7,3546	**7,3429**
4	**7,4900**	6,7391	6,6846	6,6790	**6,7167**
5	**6,6300**	6,1269	6,0638	6,0633	**6,1051**
6	**5,9900**	5,5499	5,4673	5,4565	**5,4638**
7	**5,3900**	4,9506	4,8394	4,8019	**4,7697**
8	**4,7400**	4,3464	4,2107	4,1458	**4,0755**
9	**4,0600**	3,7286	3,5666	3,4954	**3,4415**
10	**3,4000**	3,0410	2,8677	2,7953	**2,7778**
11	**2,7400**	2,3312	2,1584	2,1157	**2,0990**
12	**2,0000**	1,6918	1,5580	1,5158	**1,5058**
13	**1,5900**	1,1653	1,0935	1,0713	**1,0744**
14	**0,9500**	0,7738	0,7391	0,7214	**0,7267**
15	**0,6000**	0,4834	0,4506	0,4253	**0,4154**
16	**0,3600**	0,2508	0,2306	0,1940	**0,1792**
17	**0,1900**	0,1124	0,0885	0,0626	**0,0447**
18	**0,0600**	0,0333	0,0211	0,0106	**0,0057**
19	**0,0400**	0,0086	0,0035	0,0014	**0,0001**
20	**0**	0,0007	0,0002	0,0001	**0**
21	**0**	0	0	0	**0**
22	**0**	0	0	0	**0**

TABELA VII

FRR(%) PARA A BASE DE DADOS CASIA EMPREGANDO BUSCA POR ROTAÇÃO COM $i \in \{1, 3, 5, 7, 9\}$. (OBS.: N/D - NÃO DISPONÍVEL).

$C_{10}^{i} \rightarrow$	1	120	252	120	10
Rodadas $\rightarrow$	N/D	2	1	2	24
Total $\rightarrow$	N/D	240	252	240	240
$t_{\mathrm{RS}} \downarrow$	1 cód	3 cód	5 cód	7 cód	9 cód
1	**23,1100**	15,8923	13,889	12,9478	**12,3849**
2	**15,0900**	10,1897	8,8208	8,2403	**7,8767**
3	**10,8200**	7,1367	6,0853	5,6397	**5,3266**
4	**7,8100**	5,0909	4,2380	3,8541	**3,5994**
5	**5,8500**	3,6596	2,9825	2,7036	**2,5359**
6	**4,4200**	2,6952	2,2171	2,0435	**1,9485**
7	**3,2900**	2,0555	1,7478	1,6483	**1,5956**
8	**2,4900**	1,5549	1,3821	1,3400	**1,3001**
9	**1,6900**	1,1210	1,0265	1,0176	**0,9916**
10	**1,0900**	0,7285	0,6855	0,6940	**0,6700**
11	**0,6400**	0,4312	0,3964	0,4006	**0,3820**
12	**0,2800**	0,2225	0,1899	0,1965	**0,1855**
13	**0,1400**	0,0952	0,0768	0,0786	**0,0750**
14	**0,0300**	0,0308	0,0264	0,0253	**0,0218**
15	**0,0100**	0,0050	0,0057	0,0049	**0,0050**
16	**0**	0,0001	0,0004	0,0003	**0,0004**
17	**0**	0,0001	0	0,0001	**0**
18	**0**	0	0	0	**0**
19	**0**	0	0	0	**0**
20	**0**	0	0	0	**0**
21	**0**	0	0	0	**0**
22	**0**	0	0	0	**0**

FRR. Para $t_{\mathrm{RS}} = 1$, $i = 1$ e uma íris do olho esquerdo (exp2), obtém-se FRR = 24,34% e para $i = 9$ obtém-se FRR = 7,63%, o que representa uma redução de 16,71% na FRR.

Na Tabela IX, é feita uma comparação entre alguns sistemas de identificação biométrica de recuperação de chave criptográfica. Conforme dito anteriormente, o sistema proposto neste artigo é semelhante ao apresentado em [10], com o acréscimo do bloco de pré-processamento que gera o θ_{ref} usando a técnica de voto de maioria. Com relação

TABELA VIII

FRR(%) PARA A BASE DE DADOS NIST-ICE EMPREGANDO BUSCA POR ROTAÇÃO COM $i \in \{1, 3, 5, 7, 9\}$. (OBS.: N/D - NÃO DISPONÍVEL).

	exp1 - olho direito					exp2 - olho esquerdo				
$t_{\mathrm{RS}} \downarrow$	1 cód	3 cód	5 cód	7 cód	9 cód	1 cód	3 cód	5 cód	7 cód	9 cód
1	**21,370**	10,324	8,569	7,854	**6,757**	**24,340**	11,083	9,538	8,133	**7,632**
2	**13,750**	6,271	5,114	4,552	**4,170**	**16,170**	6,747	5,721	5,071	**4,713**
3	**9,530**	4,096	3,365	3,018	**2,724**	**11,440**	4,368	3,819	3,408	**3,230**
4	**6,970**	3,007	2,325	2,090	**2,000**	**8,730**	3,073	2,693	2,332	**2,427**
5	**5,230**	2,197	1,777	1,591	**1,526**	**6,590**	2,198	1,831	1,672	**1,779**
6	**3,830**	1,654	1,378	1,209	**1,193**	**4,890**	1,570	1,292	1,231	**1,256**
7	**2,790**	1,195	1,015	0,892	**0,887**	**3,690**	1,156	0,892	0,878	**0,823**
8	**2,150**	0,898	0,783	0,674	**0,696**	**2,690**	0,842	0,610	0,591	**0,626**
9	**1,560**	0,707	0,581	0,508	**0,546**	**1,930**	0,598	0,419	0,421	**0,425**
10	**1,160**	0,521	0,445	0,374	**0,434**	**1,380**	0,453	0,332	0,312	**0,325**
11	**0,830**	0,360	0,336	0,276	**0,327**	**0,910**	0,355	0,266	0,250	**0,246**
12	**0,620**	0,194	0,229	0,202	**0,237**	**0,630**	0,259	0,218	0,207	**0,209**
13	**0,390**	0,109	0,150	0,098	**0,188**	**0,460**	0,200	0,173	0,166	**0,173**
14	**0,240**	0,052	0,104	0,063	**0,109**	**0,350**	0,150	0,139	0,130	**0,134**
15	**0,160**	0,027	0,044	0,041	**0,052**	**0,250**	0,098	0,116	0,096	**0,100**
16	**0,120**	0,003	0,019	0,030	**0,025**	**0,180**	0,064	0,089	0,071	**0,064**
17	**0,080**	0,003	0,011	0,022	**0,011**	**0,100**	0,034	0,055	0,041	**0,032**
18	**0,050**	0	0,005	0,025	**0,005**	**0,080**	0,009	0,030	0,020	**0,007**
19	**0,040**	0,003	0,003	0,014	**0,003**	**0,030**	0	0,009	0,009	**0**
20	**0,030**	0	0	0,008	**0**	**0,010**	0	0,005	0,005	**0**
21	**0,020**	0	0,003	0,003	**0**	**0,010**	0	0	0	**0**
22	**0,010**	0	0	0	**0**	**0,010**	0	0	0	**0**

ao sistemas propostos em [13] e [14], além da técnica de pré-processamento para gerar θ_{ref}, há outras duas diferenças importantes, são elas: (a) a inserção de zeros ao invés de uma sequência pseudo aleatória [1] e (b) o uso da busca padrão ao invés da busca por rotação [10]. Por fim, o sistema proposto em [15], além das diferenças já citadas com relação aos sistemas em [13] e [14], apresenta uma esquema de correção de erro de código produto utilizando códigos de Reed-Muller.

TABELA IX

COMPARAÇÃO DE ALGUNS SISTEMAS BIOMÉTRICOS DE REGENERAÇÃO DE CHAVE CRIPTOGRÁFICA BASEADOS EM CÓDIGOS DE ÍRIS. (*) ECC - ESQUEMA DE CORREÇÃO DE ERRO UTILIZADO: A) RSH - CÓDIGO REED-SOLOMON E HADAMARD CONCATENADOS E B) RMP - CÓDIGO PRODUTO UTILIZANDO CÓDIGOS REED-MULLER.

Sistema	ECC*	Comprimento da chave (em *bits*)	FRR (%)	FAR (%)	Base de dados
Referência [13]	RSH	282	8,42	0	NIST-ICE (íris direita)
Referência [14]	RSH	128/256	0,76	0,10	NIST-ICE (íris direita)
Referência [15]	RMP	42	0,47	0	NIST-ICE (íris direita)
Referência [10]	RSH	198	0,24	0	NIST-ICE (íris direita)
Proposto	**RSH**	**222**	**0,237**	**0**	**NIST-ICE (íris direita)**

V. CONCLUSÕES

Os resultados das Tabelas VI, VII e VIII obtidos a partir das simulações usando a técnica de voto de maioria, foram realizados sempre com a busca por rotação ativada, de modo que a comparação pode ser feita com os resultados obtidos em [10]. Para todos os experimentos realizados, a taxa de falsa aceitação (FAR - *false acceptance rate*) sempre foi igual a zero para qualquer t_{RS} e para todas as bases de dados utilizadas. Destaque para a redução de 68,4% da FRR, em comparação ao resultado publicado em [10], que é obtida usando-se a base de dados NIST-ICE com $t_{\mathrm{RS}} = 1$ e o uso da técnica de voto de maioria com $i = 9$.

Na Tabela IX é possível verificar o desempenho do sistema proposto, em relação aos melhores resultados obtidos até o momento, usando as mesmas bases de dados. Ou seja, seguindo o procedimento descrito em [1], é possível recuperar chaves criptográficas com 222 *bits* com percentual de FRR de $0,237\%$ e FAR de 0% para a base de dados NIST-ICE-exp1 com $t_{\mathrm{RS}} = 12$ e usando uma única íris.

Por fim, destaca-se que a técnica de voto de maioria pode ser implementada como um pré-processamento em outros tipos de sistemas de identificação biométrica, contribuindo potencialmente para uma melhoria na identificação dos usuários.

AGRADECIMENTOS

G. N. Melo agradece a Dra. Danielle Camara por sua introdução na área de biometria e por explicar detalhes sobre as bases de dados utilizadas neste artigo. V. C. da Rocha Jr. agradece apoio parcial recebido do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq através do Projeto No. 304696/2010-2.

REFERÊNCIAS

[1] D. P. B. A. Camara, J. S. Lemos-Neto, and V. C. da Rocha Jr., "Multi-instance based cryptographic key regeneration system," *JCIS*, vol. 29, no. 1, pp. 46-55, May 2014. doi: 10.14209/jcis.2014.4

[2] A. K. Jain, P. Flynn and A. A. Ross, *Handbook of Biometrics*, Springer, 2008.

[3] S. Lin and D. J. Costello, Jr., *Error Control Coding*, Second Edition, Pearson, Prentice Hall, New Jersey, USA, 2004.

[4] S. Barra, A. Casanova, F. Narducci and S. Ricciardi, "Ubiquitous iris recognition by Médias of mobile devices," *Pattern Recognition Letters*, vol. 57, pp. 66-73, 2015. doi: 10.1016/j.patrec.2014.10.011

[5] M. F. Zafar, Z. Zaheer and J. Khurshid, "Novel iris segmentation and recognition system for human identification," *10th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, 2013, pp. 128-131.

[6] C. Narmatha and S. Manimurugan, "A new approach for iris código identification using modified contour segmentation," *IEEE International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*, Coimbatore, India, March 2014, pp. 1-7. doi: 10.1109/ICGCCEE.2014.6921399

[7] A. Mallikarjuna and S. Madhuri, "Biometric security techniques for IRIS recognition system," *IJRCCT*, vol. 2, no. 8, pp. 589-593, 2013.

[8] J. Bringer, C. Morel and C. Rathgeb, "Security analysis of Bloom filter-based iris biometric template protection," *International Conference on Biometrics (ICB)*, Phuket, 2015, pp. 527-534.

[9] K. Nandakumar and A. K. Jain, "Biometric template protection: bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88-100, Sept. 2015. doi: 10.1109/MSP.2015.2427849.

[10] G. N. Melo, V. C. da Rocha Jr. and J. S. Lemos-Neto, "User identification and key regeneration system employing rotated reference códigos of the iris," *JCIS*, vol. 31, no. 1, pp. 60-68, May 2016. doi: 10.14209/jcis.2016.5

[11] "BioSecure Network of Excellence", Disponível em: http://www.biosecure.info. Acesso em: 21 de Março de 2016.

[12] National Institute of Science and Technology (NIST), "Iris Challenge Evaluation," 2005, Disponível em: http://iris.nist.gov/itl/iad/ice.cfm. Acesso em: 21 de Março de 2016.

[13] S. Kanade, D. P. B. A. Camara, E. Krichen, D. Petrovska-Delacrétaz and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," *The 6th Biometrics Symposium 2008 (BSYM2008)*, Tampa, Florida, USA, 2008, pp. 59-64. doi: 10.1109/BSYM.2008.4655523

[14] S. Kanade, D. P. B. A. Camara, D. Petrovska-Delacrétaz and B. Dorizzi, "Application of biometrics to obtain high entropy cryptographic keys," *Proceedings of World Academy of Science, Engineering and Technology*, vol. 27, Hong Kong, China, March 2009, pp. 251-255.

[15] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zmor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 4, pp. 673-683, 2008. doi: 10.1109/TIFS.2008.2002937.