Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Error Free Watermarked Approach Using Fuzzy Correction Code

Bhupendra Kumar
Research Scholar Mewar University,
Chittorgarh, Rajsthan, India

Deo Brat Ojha
Professor, Department of Mathematics,
Mewar University, Chittorgarh, Rajsthan, India

Abstract— In this article, We propose a combined approach of cryptography with LSB-DWT watermarking to secure biometric templates. The key-binding bio-cryptosystem is based on fuzzy sketches that handle intra-class variability by using error correction codes. Fuzzy correction code are used to account for errors that occur in iris codes. The proposed system was also capable of withstanding minor spatial and frequency watermarking attacks without major degradation in the performance.

Keywords— Biometrics, Biometric Templates, Fuzzy error correction code.

I. INTRODUCTION

The necessity of fast and secure diagnosis is vital in the medical world to save the life of world creature. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net [3, 4, 5]. For image transmission, two different approaches of technologies have been developed. The first approach is based on content protection through encryption [1], [2]. In this approach, proper decryption of data requires a key. The second approach bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. In the current era, the transmission of Image over internet is so much challenging over the internet. In this manner, the better way to transmit the image over internet is encryption. Using the cryptography we secure the image as well as also better utilization of the communication channel with compression technique. Cryptography is a tool of security that aims to provide security in the ciphers of any kind of messages. Cryptographic algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [2]

McEliece proposed the first public-key cryptosystem (the McEliece Scheme) based on algebraic coding theory in 1978[1]. The idea behind McEliece public-key cryptosystem is based on the fact that the decoding problem of an arbitrary linear code is an NP-hard problem [2].The McEliece scheme has the advantage of high speed encryption and decryption and this system employs probabilistic encryption [1,2], which is better than other type of deterministic encryption[6] in preventing the elimination of any information leaked through public-key cryptography[7,8,9,10]. It is point of remark [6] that the security comparison is made here for classical attackers. The picture changes drastically to the advantage of the McEliece system if we consider two systems.

It is point of remark [6] that the security comparison is made here for classical attackers. The picture changes drastically to the advantage of the McEliece system if we consider two systems. to offer the same level of security if breaking them requires quantum computers with the same number of qubits. This cryptosystem cannot be used for authentication because the encryption is not one to one and total algorithm is truly asymmetric. The rest of the paper is organized as follows: in Section 2, related work in the area of combining biometrics with cryptography is summarized. The proposed algorithm for cryptographic key binding using iris code and a description of the watermarking algorithm used and the detailed steps is given in Section 3. Section 4 concludes this paper.

II. RELATED WORK

Although template security is gaining interest in the research field, most of those efforts focused on fingerprint and face templates. And the motives for watermarking was to detect any tampering with the original template [23] or using one template to watermark another template [2],[12],[15],[24] which provides multimodal authentication, as well as, template protection.

Ratha et al. [8] introduced the idea of "cancelable biometrics" to refer to the scheme of storing a distorted biometric template instead of the actual one. These "distortions" or transformations depend on parameters that can be changed, if the database is compromised and a new set of "templates" need to be issued. Iris recognition [16] has proven very stable and suitable for large scale application [21].[22]. Iris template protection, however, is still an emerging research point especially revocable iris templates. A way to provide revocability was suggested in [29], in which a user specific key is used to determine a reference bit in the iris template. All rows in the template are then connected end-to end to form a roll. Another method was suggested in [31], in which a user specific key determined shifts as well as combinations of rows in the template. Kanadeet. al [30] proposed an iris template shuffling algorithm that was adopted in this paper and is discussed later in details.

Key-Generating

Monrose et al. [6] where among the first to address biometric key generation by using key stroke dynamics and later voice features [9] to create a hardened password. Davida et al. [4],[5] were the first to propose an algorithm for template protection based on the iris biometric. An [N,K,D] bounded distance error-correcting code is then constructed resulting in an N-bit codeword, denoted by T||C. The codeword is hashed and digitally signed, and together with the check bits C, stored as the database template for the user.

Key-Binding

In their "fuzzy commitment"" scheme [7], Juels and Wattenberg suggest that the user at the enrollment time selects a secret message c from a set of codewords of some error-correcting code. To commit to a value x, the user computes an offset of the form d=c-x. The commitment then consists of the pair (d; h(c)). To decommit using key x', the user computes d+x' and, if possible, decodes to the nearest codeword c'. The decommitment is successful if h(c')=h(c). Shielding functions were suggested by Tylus et al. [13],[14], [20] for template protection. They assumed that a noise-free template X is available at the enrollment time and use it to enroll a secret K to generate a helper data P. In their implementation the authors assume that each dimension of the template is quantized at q resolution levels. In each dimension, the process of obtaining P is equivalent to finding residuals that must be added to X to fit to odd or even grid quantum depending upon whether the corresponding K bit is zero or one. At decryption time, the "noisy" biometric template X' is used to decrypt and obtain a decrypted message K', which is approximately the same as K. It is hoped that the relatively few errors in K' can be corrected using error-correction techniques.

Dodis et al. [17] formalized the idea of using error correction codes to deal with inter-user variablities. They introduced the terms secure sketch and fuzzy extractors. These methods hope that without knowledge of the "original" message or template in our case and given the helper data P, we'll be able to "retrieve" a key k. Juels and Sudan's fuzzy vault scheme [11] is one of the most popular algorithms implemented for fingerprint template protection. During Enrollment a key is used to determine the coefficients of an n-degree polynomial. The unordered feature set is then evaluated at the polynomial. Points that don't lie on the polynomial are then added as chaff points and added to the genuine point set to form the fuzzy vault. To "unlock" a vault a sample template is acquired and used together with the fuzzy vault to try to estimate at least (n+1) genuine points so reconstruction of the polynomial through Lagrange interpolation would be possible. If successful, coefficients of the polynomial should match the stored key.

Hao et al. [25] proposed a different key-binding iris template protection scheme, in which a random key is entered into a coding module to generate a 2048 bit string adapted to the Daugman's iris code length [12]. The encoder also includes random (Hadamard) and burst (Reed Solomon) error correction codes to compensate for the fuzziness of biometric templates. The choice of the error correction coding parameters was based on studying the errors in iris code and the genuine and imposter distributions. During authentication, the acquired iris template in encoded the same way. By using error correction, a simple comparison between the acquired and the original keys serves as the authentication and decision making module.

Watermarking

Watermarking in the transform domain is more robust than the spatial domain and is usually chosen for watermark embedding. Fast Fourier Transform (FFT) was, for example, chosen in [26] to exploit image properties. They used a normalized segmented iris image as a watermark and a face image as the cover work. The Discrete Cosine Transform (DCT) was chosen in [18] as a classic and popular domain for image processing. The sensitivity of the human visual system to the DCT basis images has been extensively studied, which resulted in the recommended JPEG quantization table [4]. These results can be used for predicting and minimizing the visual impact of the distortion caused by the watermark [4] and, hence permit the embedding of more robust watermarks.

Another possible transform for watermark embedding is that of the wavelet domain. One of the many advantages of the wavelet transform is that it is believed to more accurately model aspects of the HVS (Human Visual System) as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive, such as the high-resolution detail bands, at little to no additional impact on image quality[4]. In [19] the authors compared 4 watermarking techniques used to embed an iris template into a face cover image. The four techniques they chose were LSB substitution, Modified Correlation Based Algorithm (MCBA), Modified 2D DCT (M2DCT), and DWT. Robustness of all four algorithm was tested against Jpeg compression, Gaussian noise addition, median filtering, blurring, gamma correction, file format conversion, and printing and rescanning of the watermarked image. As in all other biometric watermarking systems, robustness is measured by the recognition accuracy. In their experiments transform domain watermarking as expected performed better in withstanding different types of attacks, with DWT performing best in most cases, followed by the M2DCT and then MCBA. LSB substitution again, as expected, performed worst especially after Jpeg compression where the watermark was completely lost.

III. PROPOSED SYSTEM

Error Correction Code:

A metric space is a set C with a distance function dist : $C \times C \to R^{+} = [0, \infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points)[12].

Definition : Let $C\{0,1\}^n$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by $dist(c_i, c_j) = \sum_{r=1}^{n} |c_{ir} - c_{jr}| \qquad c_i, c_j \in C$ This is known as Hamming distance [12].

Definition : An error correction function f for a code C is defined as $f(c_i) = \{c_j / dist(c_i, c_j)$ is the minimum, over $C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i [12].

Definition : The measurement of nearness between two code words c and c' is defined by nearness $(c, c') = dist(c, c') / n$, it is obvious that $0 \leq$ nearness $(c,c') \leq 1$[12].

Definition : The fuzzy membership function for a codeword c' to be equal to a given c is defined as[12]

$FUZZ(c') = 0$ if nearness$(c, c') = z \leq z_0 < 1$

$= z$ otherwise

Watermarking:

Usually, image watermarking is performed using Discrete Wavelet Transform (DWT) because DWT preserves frequency information in stable form and allows good localization both in spatial and frequency domain [1]. In this paper we combine the traditional DWT and LSB substitution algorithm to achieve robustness against both geometric and frequency watermarking attacks.[27],[28]

Watermark Embedding Algorithm:

Step 1: Three-level Discrete Wavelet Transform (DWT) is applied to the original cover image I. Because the approximation band carries the most sensitive coefficients (to the human visual System) and the diagonal approximation band carries the least significant ones (most vulnerable to image processing attacks), the coefficients of the vertical and horizontal band are chosen for watermark embedding. Only the second and third levels of DWT are used for embedding because these two levels provide more resilience to geometric and frequency attacks.

Step 2: In the detailed sub-bands coefficients are chosen according to a user specific key. Since the watermark will be embedded in 4 sub-bands, p is ◆ of the watermark length. The watermark is embedded 5 times to increase robustness. After choosing the positions of the coefficients to be watermarked, they are adjusted according to the following equation:

Step 3: After embedding, Inverse Discrete Wavelet Transform (IDWT) is applied to the watermarked coefficients to generate the secured watermarked cover image.

Watermark Extraction Algorithm:

Step 1: Similar to embedding, three-lever Discrete Wavelet Transform (DWT) is applied to the original cover image I to obtain the 2nd and 3rd level detail bands.

Step 2: The user specific key is used to determine the watermark embedding locations in the same manner as in the embedding process. From each coefficient a watermark is extracted from the 5th least significant bit of the coefficient.

Step 3: For each 5 bits of extracted watermark, majority decoding is used to determine the equivalent extracted watermark bit. The extracted bits are then arranged to form the locked iris code.

Step 4: The extracted locked iris code is then xored with the extended sample iris code.

Procedure for detecting and correcting error

If any error occurred during the transmission of message, we can detect and correct using fuzzy error correcting code.

Receiver check that $dist(t(c)c') > 0$, he will realize that there is an error occur during the transmission. Receiver apply the error correction function f to $c' : f(c)$.

Then receiver will compute nearness $(t(c), f(c')) = dist(t(c) f(c')) / n$

$FUZZ(c') = 0$ if nearness$(c, c') = z \leq z_0 < 1$

$= z$ otherwise

IV. CONCLUSION

With the increased use of biometric systems, the possibility of attacks on the template database also increases. in the error correction module there is a tradeoff between key length and performance of the system. The watermarking scheme suggested does not affect the performance of the iris recognition system. Attacks on the watermarked image slightly affect the false acceptance rate and increase the false reject rate, but still within very acceptable limits that does not degrade the performance of the system.

REFERENCES

[1]. R.J.McEliece, " A public-key cryptosystem based on algebraic coding theory," DSN Progress Report,42-44,1978,pp.114-116.

[2]. E.R.Berlekemp, R.J.McEliece, and H.C.A. vanTilborg, " On the inherent intractability of certain coding problems," IEEE Transactions on Information Theory, vol.24, No.5, 1978, pp.384-386.

[3]. G. Lo-varco,W. Puech, and M. Dumas. "Dct-based watermarking method using error correction codes", In ICAPR'03, International Conference on Advances inPattern Recognition, Calcutta, India, pages 347–350, 2003.

[4]. R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. "Confidential storage and transmission of medical image data", Computers in Biology and Medicine, 33:277–292, 2003.

[5]. Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and RudineiGoularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department, Maringa, PR, Brazil.

[6]. Johannes Buchmann, Carlos Coronado, Martin D¨oring, Daniela Engelbert,Christoph Ludwig, Raphael Overbeck, Arthur Schmidt ,Ulrich Vollmer, Ralf-Philipp Weinmann , "Post- Quantum Signatures",eprint.iacr.org/2004/297.

[7]. Ramveer Singh , Awakash Mishra and D.B.Ojha "An Instinctive Approach for Secure Communication – Enhanced Data Encryption Standard (EHDES)" International journal of computer science and Information technology, Vol. 1 (4) , 2010, 264-267.

[8]. D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati Garg "An Innovative Approach to Enhance the Security of Data Encryption Scheme" International Journal of Computer Theory and Engineering, Vol. 2,No. 3, June, 2010,1793-8201.

[9]. J.P.Pandey, D.B.Ojha, Ajay Sharma, "Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

[10]. O. Rioul, M. Vetterli, "Wavelets and signal processing", IEEE Signal Processing Magazine, vol. 8(4), pp. 14-38., 1991.

[11]. Lin H. and Anil. K.J., "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998

[12]. G. Voyatzis, N. Nikolaidis, I. Pitas, "Digital Watermarking: An Overview", 9th European Signal Processing Conference (EUSIPCO'98), 1998.

[13]. G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through online biometric identification" in Proc. 1998 IEEE Symposium on Privacy and Security, pp. 148-157, May 1998.

[14]. G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an offline biometric based identification scheme," in Proceedings of the Workshop of Coding and Cryptography, pp. 129-138, 1999.

[15]. F. Monrose, M. K. Reiter, and S. Wetzel. "Password hardening based on keystroke dynamics", In Proceedings of the 6th ACM conference on Computer and Communications Security, pages 73-82, November 1999.

[16]. A.Juels and M.Wattenberg, "A fuzzy commitment scheme," CCS 1999: Proceedings of the 6th ACM conference on Computer and communications security, pp. 28-36, 1999.

[17]. Ratha, N. and Connell, J., "Cancelable Biometrics", presented at Biometric Consortium 2000 Conference, Sept. 13-14, 2000.

[18]. F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. "Cryptographic key generation from voice", In Proceedings of IEEE Symposium Security & Privacy, pp. 202-213, 2001.

[19]. I.J. Cox, M. Miller, J. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.

[20]. A. Juels and M. Sudan. "A fuzzy vault scheme", A. Lapidoth and E. Teletar, editors, Proc. IEEE International Symposium on Information Theory, page 408, 2002.

[21]. J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, pp. 1148-1161, Nov. 1993.

[22]. Linnartz, J.P., Tuyls, P.: "New shielding functions to enhance privacy and prevent misuse of biometric templates". In Proceedings of the 4th International Conference on Audio and Video Based Biometric Person Authentication, Guildford, UK, pp. 393-402, 2003.

[23]. Verbitskiy, E., Tuyls, P., Denteneer, D., Linnartz, J.P.; "Reliable biometric authentication with privacy protection". In: Proceedings of the 24th Symposium on Information Theory in the Benelux, Veldhoven, The Netherlands, 2003.

[24]. Anil K. Jain, UmutUludag, "Hiding Biometric data", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vo1.25, No.ll, November 2003.

[25]. J. Daugman, "How iris recognition works", IEEE Transactions on Circuits Systems and Video Technology, vol.14, pp.21-30, 2004.

[26]. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, in Lecture Notes for computer Science, vol. 3027, Springer, 2004.

[27]. M. Vatsa, R. Singh, P. Mitra, A. Noore, "Digital watermarking based secure multimodal biometric system", IEEE International Conference on Systems, Man and Cybernetics, Vol. 3, pp: 2983- 2987,October 2004.

[28]. M. Vatsa, R. Singh, P. Mitra, A. Noore, "Comparing robustness of watermarking algorithms on biometrics data", Proceedings of the Workshop on Biometric Challenges from Theory to Practice - ICPR Workshop, pp. 5-8, 2004.

[29]. P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. "Practical Biometric Authentication with Template Protection", Proceedings of Fifth International Conference on Audio-and Video-based Biometric Person Authentication, pp. 436-446, July 2005.

[30]. A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security: Challenges and Solutions", Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.

[31]. J. Daugman, "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons", Proceedings of the IEEE, vol.94, pp.1927-1935, 2006.

