Strengthen Fingerprint Data Security Using Chaotic Map Approach

Ankit Jat, Prof. Sandeep Raghuwanshi

1Scholar, M.TECH .Information Technology
Samrat Ashok Technological Institute, Vidisha 464001 (M.P), India

2Assistant professor, Information technology,
Samrat Ashok Technological Institute Vidisha 464001 (M.P), India

Abstract: A data security is an issue for research from the beginning. Different method and different technique have been implemented for data security but no one gives the high security provides for data. it can be use the chaotic map technique for data security. The salient features of the technique is that any authorized user can retrieve the corresponding fingerprint information from the complex encrypted and multiplexed image by a single decryption process with the authentic key. An orthogonal coding scheme with chaotic map is developed to encrypt the given fingerprint image. In this paper, we presented a new algorithm of encryption and decryption of images. The algorithm is based on the concept of shuffling the pixels positions and changing the gray values of the image pixels. To perform the shuffling of the plain-image's pixels, a block based shuffling scheme is proposed, in which the plain-image is decomposed into 8x8 size blocks and a 2D Cat map is applied in three different ways to achieve good shuffling effect. Moreover, the control parameters of shuffling are randomly generated using a 2D Standard map to enforce the secrecy of the image. The encryption of the shuffled image is done using chaotic sequence generated through a 2D standard map. A traditional cryptosystems employ algorithms where confusion and diffusion are linear function of the number of iteration and key length. All the simulation and experimental analysis show that the proposed image encryption system has a very large key space, high sensitivity to secret keys. The proposed cryptographic technique involves a simple architecture by not requiring any mathematical transformation. Performance of the technique is investigated through computer simulation employing real-life fingerprint images.

Keywords- biometric features, cryptography, orthogonal coding, multiplexing, chaotic map.

I. INTRODUCTION

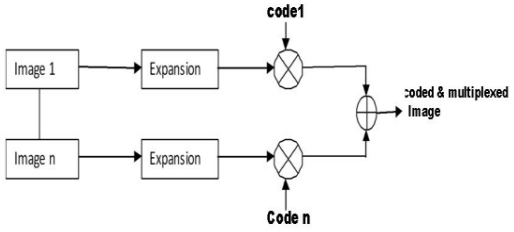
Biometric features, including face, fingerprint, iris, have been found to be unique for any human and hence been proposed to be utilized as an efficient mean to establish the identity of a person. A considerable amount of research interest has been developed to devise biometric recognition techniques for a wide range of applications, including border security, authentication, identification, verification, protection of identity theft, and so on[1][4][16]. However, the major challenge of biometric recognition systems is to secure the biometric features from any unauthorized access, information leakage, and compromise or modification. Biometric cryptosystems have the requirement of encrypting the feature, securely storing the information and also of faithfully reproducing the feature for authentication or identification purpose[6]. Optical image processing techniques have offered efficient information security and fraud prevention systems. A couple of optical encryption methods have so far been proposed in the literature[2][18], including double phase encoding scheme using joint transform correlation (JTC)[3][11],exclusive-or encryption[26]security verification using polarization-encoded mask[27], multiplexed minimum average correlation energy phase-encrypted filter[28],and fractional Fourier transformation[29].However, majority of the techniques employ a pseudo-random number for encoding purpose. Since these numbers are not totally uncorrelated from one another, the security is not strong enough to prevent a wrong code from being able to extract some of the features of the coded information. The objective of this paper is to develop a novel algorithm for securing fingerprint information. a given fingerprint image is encrypted using a orthogonal coding scheme which provides zero cross-correlation between the code words[2]. The salient features of the proposed technique are that it involves a simple architecture requiring no complex mathematical transformation and additionally multiple encrypted information can be multiplexed together to save storage and/or transmission bandwidth. Computer simulation investigation verifies that the confidential fingerprint information can be retrieved successfully without any loss or distortion provided the correct code is applied.

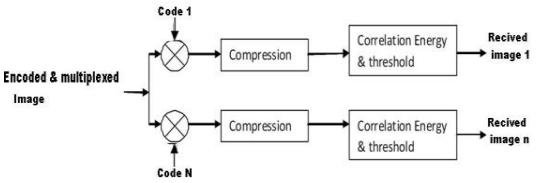
II .ANALYSIS

Figure 1 shows the block diagram of the proposed security system for fingerprints. First, the given fingerprint images are encoded using individual orthogonal code. The input images are expanded in one dimension and then multiplied by the respective code as shown in Fig. 1(a). Then, the individual encoded images are superimposed on a common spatial domain. Let $ti(x, y)$ be the expanded form of the i'th

fingerprint image *fi*(*x, y*), and *ci*(*x, y*) is the respective code. Thus the encoded and multiplexed image can be expressed

$$S(x, y)=\sum_{i=1}^{N} c_i(x, y)t_i(x, y) \quad \ldots\ldots\ldots(1)$$





Among different orthogonal coding teccode is employed in the paper, which applying the Hadamard transform repeatedly as described below

$$H_1 = [0] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

$$H_{2n'}=\begin{bmatrix} Hn & Hn \\ Hn & Hn \end{bmatrix} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

The set of encryption keys are generate a square matrix, where the length of power of 2. The length of the code corresponding to the number of independent codes. As shown in Fig. 1(b), the required information can be retrieved from encrypted image by simply multiply respective code. Then a threshold performed where an appropriate value is selected based on the format of the set used. If *ci* (*x,y*) represents the address code for the *i*tch fingerprint to be decrypted, then the after the correlation operation performed received signal can be expressed as

$$d(x,y)=\int_{\infty}^{N}\int \left[\sum_{k=1} C_k(u,v)T_k(u,u)\right] Ci(u-x,v-y)dudv \quad \ldots\ldots\ldots\ldots(4)$$

where *C*(*u, v*) and *T*(*u, v*) are the Fourier the spatial domain signals, *c*(*x, y)* and T(x,y) respectively. It can be obvious from eq.(4) the desired decrypted fingerprint will be the output after the threshold operation, because other fingerprint will contribute nothing as the cross the any two different codes is zero. The demultiplexing operation performed during correlation processing is required for this purpose

III. CHOATIC MAP

Nowadays, communication networks such as mobile networks and the Internet are well developed. However, they are public networks and are not suitable for the direct transmission of confidential messages. To make use of the communication networks already developed and to keep the secrecy simultaneously, cryptographic techniques need to be applied. Traditional symmetric ciphers such as Data Encryption Standard (DES) are designed with good confusion and diffusion properties[30].These two properties can also be found in chaotic systems which are usually ergodic and are sensitive to system parameters and initial conditions. In recent years, a number of chaos-based cryptographic schemes have been proposed. Some of them are based on one-dimensional chaotic maps and are applied to data sequence or document encryption[31][32].For image encryption, two-dimensional (2D) or higher-dimensional chaotic maps are naturally employed as the image can be considered as a 2D array of pixels[33][25].I suggested that a chaos-based image encryption scheme should compose of two processes: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with a 2D chaotic map while the latter alternates the value (gray-level) of each pixel in a sequential manner. This architecture formed the basis of a number of chaos-based image ciphers proposed subsequently.Therefore they suggested using a standard map for confusion while keeping the logistic map for pixel value diffusion. To achieve a satisfactory level of security, recommended performing four overall rounds of confusion and diffusion[24] .In each confusion stage, 4 permutation rounds should be performed. These lead to a total of 16 permutation rounds and 4 diffusion rounds. Although measures such as pre-computation of permutation mode and sine table were 3 suggested to reduce the computational complexity, the relatively slow diffusion process still limits the performance of this cryptosystem. To accelerate the encryption speed of cryptosystem and other ciphers based on the iterative confusion-diffusion processes, we propose to introduce certain diffusion effect in the confusion process so that this effect is not solely contributed by the slow diffusion process. Simulation results show that the number of overall rounds and hence the number of time-consuming diffusion processes is reduced without sacrificing The security level. The overall encryption time is shortened although the time required in the confusion stage is increased slightly. The paper is organized as follows. In the next section, the architecture of cryptosystems based on iterative confusion-diffusion processes is introduced with Lian *et al*'s scheme as an example. The design concept of our approach is described in. Simulation results and performance analyses are reported in. In the last section, a conclusion is drawn.

Architecture of Chaos-based Image Cryptosystems:

typical architecture of the chaos-based image cryptosystems is

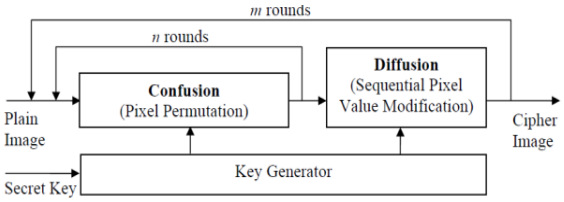


fig. Typical architecture of the chaos-based image cryptosystems

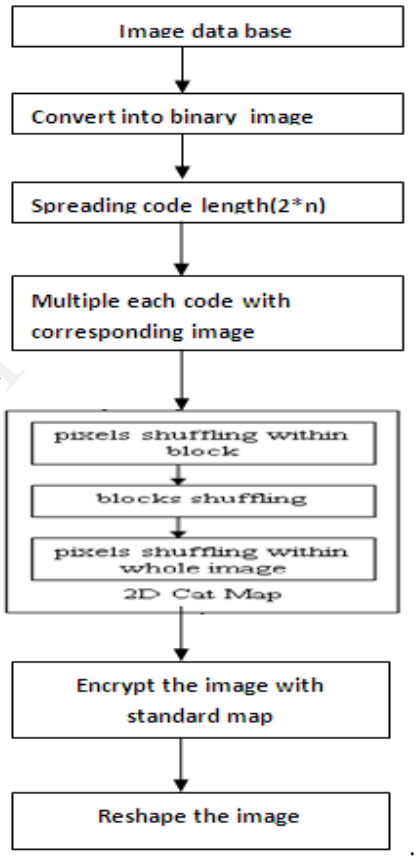
There are two iterative stages in the chaos-based image cryptosystem. The confusion stage permutes the pixels in the image, without changing its value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image. To decorrelate the There are two iterative stages in the chaos-based image cryptosystem. The confusion stage permutes the pixels in the image, without changing its value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image. To decorrelate the relationship between adjacent pixels, there are n permutation rounds in the confusion stage with $n \geq 1$. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The parameters of the chaotic maps governing the permutation and the diffusion should better be different in different rounds. This is achieved by a round key generator with a seed secret key as input.
In Lian *et al*'s cryptosystem[24] , the confusion process is realized solely by permuting pixel positions without pixel value mixing. It employs an invertible discretized 2D standard map with the introduction of random scan couple (rx, ry) for corner-pixel confusion, as given by.

$$X_{K+1} = (x_k + y_k + r_x + r_y) \bmod N$$
$$Y_{k+1} = (y_k + r_y + k_c \sin 2\prod X_{K+1}/N) \bmod N$$

where (xk, yk) and (xk+1, yk+1) is the original and the permuted pixel position of an $N \times N$ image, respectively. The standard map parameter KC is a positive integer.

IV. The Proposed Scheme

The proposed image encryption algorithm has two major steps. Firstly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. To achieve this, a block based image shuffling scheme is proposed using 2D Cat map. Then the pixel values of the shuffled image are encrypted by employing a 2d standard map. The periodicity of Cat map degrades the security, because the possible attack may iterate the map continuously to reappear the plain-image, this makes the Straight forward use of conventional Cat map unsafe for image security. To withstand the periodicity attack of Cat map, a new block based image shuffling scheme using Cat map is proposed in which the two control parameters a, b of map are randomly generated through a key dependent chaotic sequences. The control parameters of Cat map are the control parameters of shuffling. The shuffling effect obtained after a number of iterations depends on these parameters.



V. **Experimental Result**

Encryption of image :

Data base size	Spreading length(2*n)	Standard size	H/W ratio	Encryption key	Enc.Time
4	8	64	4	659	0.35265
4	8	128	4	659	0.49581
4	8	256	4	659	1.4255

Table 1. Encryption of image

Decryption of image:

Image no.	Decryption key	Decryption time
2	659	0.11291
2	659	0.15989
2	659	0.27194

Table 2.Decryption of image

VI. CONCLUSION

An efficient fingerprint Security system is proposed in this paper employing orthogonal coding scheme. The technique has been found to provide an efficient and successful encryption, multiplexing and decryption performance. It provide with excellent security features with a very simple architecture. The technique can also be implemented optic to yield an effective real-time security system.

In this paper, we presented a new algorithm of encryption and decryption of images. The algorithm is based on the concept of shuffling the pixels positions and changing the gray values of the image pixels. To perform the shuffling of the plain-image's pixels, a block based shuffling scheme is proposed, in which the plain-image is decomposed into 8x8 size blocks and a 2D Cat map. Hence, we can say that all the analysis prove the security, effectivenees and robustnesss of the proposed image encryption algorithm

(1)

(2)

(3)

(4)

Encryption fingerprint image , decryption fingerprint image

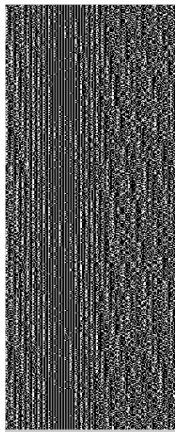


image no-2

REFERENCES

[1] B. Chen and V. Chandran, "Biometric template security using higher order spectra," *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1730 – 1733, 2010.

[2] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Transactions on Information Theory*, vol. IT-35, vol. 595 604, 1989

[3] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Optical Engineering*, vol.39, no. 8, pp. 2031–2035, 2000.

[4] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain,"Biometric cryptosystems: issues and challenges, *Proceedings of the IEEE*, vol. 92, pp. 948-960, 2004.

[5] C. L. Nikias and J. M. Mendel, "Signal processing with higher-order spectra," *Signal Processing Magazine,IEEE*, vol. 10, pp. 10-37, 1993

[6] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems,"*IBM Systems Journal*, vol. 40, pp. 613-634, 2001.

[7] V. Chandran, B. Carswell, B. Boashash, and S. A. Elgar, "Pattern recognition using invariants defined from higher order spectra: 2-D image inputs," *IEEE Transactions on Image Processing*, vol. 6, pp. 703-712, 1997.

[8] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 2005;26(1):117-29.

[9] Feng Y, Li LJ, Huang F. A symmetric image encryption approach based on line maps. In: Proc ISSCAA 2006, Jan 2006, p. 1362-67.

[10] V. Chandran and S. L. Elgar, "Pattern Recognition Using Invariants Defined From Higher Order Spectra- One Dimensional Inputs," *IEEE Transactions on Signal Processing*, vol. 41, p. 205, 1993

[11]Rodolfo ,H. Rajbenbach, and J.-P. Huignard, ''Performance of a photorefractive joint transform correlator for fingerprint identification,''*Opt. Eng.* **34**, 1166–1171 ~1995!.

[12]C. L. Wilson, C. I. Watson, and E. G. Paek, ''Combined optical and neural network fingerprint matching,'' *Proc. SPIE* **3073**, 373–382~1997!.

[13]A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006..

[14] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *IEEE Transactions on Systems, Man and Cybernetics Part C*, vol. 35, no. 3, pp. 335–343, 2005.

[15] A. Ross, J. Shah, and A. K. Jain, "From template to image: reconstructing fingerprints from minutiae points," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544–560, 2007.

[16] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '04)*, vol. 3, pp. 2203–2206, Taipei, Taiwan, June 2004..

[17] J. C. Yen and J. I. Guo, "A new chaotic key-based design for image encryption and decryption." in Proceedings of IEEE International Symposium on Circuits and Systems, Vol.4, pp. 49–52, 2000..

[18] Y. H. Doh, J. S. Yoon, K. H. Choi, and M. S. Alam, "Optical security system for the protection of personal identification information," *Applied Optics*, vol. 44, no. 5, pp. 742–750, 2005.

[19] L. Zhang, X. Liao, X. Wang, "An image encryption approach based on chaotic maps." Chaos, Solitons and Fractals, vol. 24, no. 3, pp. 759–765, 2005..

[20] C. Dongming, Z. zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists, pp. 2792-2796, 2008.

[21]Fridrich J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Int. J. Bifurcat Chaos 1998;8(6):1259-84

[22] Pareek NK, Patidar V, Sud KK. Discrete chaotic cryptography using external key. Phys Lett A 2003;309:75-82.

[23] Belkhouche F, Qidwai U, Gokcen I, Joachim D. Binary image transformation using two-dimensional chaotic maps. In: Proc ICPR 2004, Aug 2004, p.823-6.

[24] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 2005;26(1):117-29.

[25]Lian SG, Sun J, Wang Z. Security analysis of a chaos-based image encryption algorithm, Physica A 2005;351:645-61.

[26]B. Javidi, L. Bernard and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," *Optical Engineering*, vol. 38, no. 1, pp. 9 – 19, 1999.

[27] B. Javidi and T. Nomura, "Polarization encoding for optical security systems," *Optical Engineering*, vol. 39, no. 9, pp. 2439–2443, 2000

[28] Y. H. Doh, J. S. Yoon, K. H. Choi, and M. S. Alam, "Optical security system for the protection of personal identification information," *Applied Optics*, vol. 44, no. 5, pp. 742–750, 2005.

[29] Y. Zhang, C. H. Zheng, and N. Tanno, "Optical encryption based on iterative fractional Fourier transform," *Optics Communications*, vol. 202, pp. 277–285, 2002.

[30] Schneier B. Cryptography: Theory and Practice. Boca Raton: CRC Press; 1995.

[31] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240(1-2):50-4.

[32] Pareek NK, Patidar V, Sud KK. Discrete chaotic cryptography using external key. Phys Lett A 2003;309:75-82.

[33] Fridrich J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Int. J. Bifurcat Chaos 1998;8(6):1259-84.