Economic Affairs, Vol. **69**(02), pp. 809-816, June 2024
DOI: 10.46852/0424-2513.3.2024.4

AESSRA

RESEARCH PAPER

Enhancing Financial Security: Chaotic Map Integration with Biometric Data

Durgabati Podder* and Subhrajyoti Deb

Department of Computer Science and Engineering, ICFAI University Tripura, India

Corresponding author: subhrajyotideb1@gmail.com (**ORCID ID:** 0000-0001-6939-0113)

Received: 12-01-2024 **Revised:** 27-02-2024 **Accepted:** 06-03-2024

ABSTRACT

As a digitalization of attendance systems and identity authentication systems at places like factories, airports, educational institutions, healthcare centers, etc. They contain a lot of biometric data like fingerprints, so there is a high risk of data breaches from the databases used by the authentication centers. The biometrics are less costly to upkeep, so it is very economical. The biometric data is susceptible, and sometimes attackers may use it to cause financial damage using these biometric data, as they are used in many government identity cards as proof. Due to this, it becomes essential to protect these data. Research communities have proposed many image security solutions to prevent security breaches. Unfortunately, many cryptosystems today have excessive computational complexity and inadequate security. Thus, protecting these biometric image data and lowering computing complexity are the primary goals of our work. So we have proposed an encryption technique which contain dual confusion followed by a diffusion process. For the first part of confusion, we have designed a divide-rotate algorithm and for the second phase, we have developed a pixel shifting algorithm. A pseudo-random sequence generator is used to generate a chaotic range of values and diffuse the image, and in this process, a Logistic map is used. Studies on security and performance show that the suggested approach has a high degree of randomness and is resistant to statistical entropy-based, differential as well as brute-force attacks. From the analysis and findings, it is clear that the suggested method is incredibly sensitive, financially trustworthy, and performs better than other similar state-of-the-art systems, all with reduced computing complexity.

HIGHLIGHTS

- Using a chaotic map, protect the biometric data against financial fraud.
- In order to protect the fingerprint data financially, an encryption technology has been developed.
- Dual confusion is the first step of the encryption technique, and is followed by a diffusion process.
- To achieve dual confusion, two algorithms have been developed: divide-rotate and pixel shifting.
- A top-notch generator of pseudo-random sequences generated on the Logistic map was used to disperse the permuted image pixels.

Keywords: Biometric data, Fingerprint, Image Encryption, Confusion, Diffusion, Financial Security, Logistic map

In essence, biometric systems are pattern recognition systems that work by using a person's distinct biological and personal traits to verify information. They make advantage of both personal and physical characteristics, including voice recognition, keyboard patterns, handwriting patterns, fingerprints, iris sequences, and face recognition and hand geometry. According to Natgunanathan *et al*. (2016), there are several privacy benefits associated with biometric recognition. For instance, biometrics can eliminate the need to memorize multiple passwords and pin numbers, saving you the trouble. Additionally, biometrics can be used to prevent unauthorized people from accessing computers, mobile devices,

How to cite this article: Podder, D. and Deb, S. (2024). Enhancing Financial Security: Chaotic Map Integration with Biometric Data. *Econ. Aff.*, **69**(02): 809-816.

Source of Support: None; **Conflict of Interest:** None

government facilities, bank ATMs, workplaces, etc. Furthermore, the same biometric information can be applied universally and uniformly. Two categories can be used to categorize biometric data: physiological characteristics DNA, face, hand geometry, fingerprints, iris, and retina; behavioral characteristics, such as voice, gait, and signature. Regular sampling is required since an individual's behavioral characteristics may vary over the course of their life. Comparatively, substantially less sampling is needed for physiological biometric data.

Biometric systems make it possible to easily identify someone based on their physical or behavioral traits as discussed by Dunstone and Yager (2009). They establish a direct connection between identities and owners as opposed to traditional token-based or knowledge-based systems. Furthermore, it is difficult to relinquish or forget these identities. Over the last ten years, biometric methods have grown in popularity and are being used in a variety of contexts, such as government and banking institutions, retail establishments, law enforcement, healthcare facilities, and airport/border controls. Companies like Apple and Samsung have added biometric features to their most recent smart phones in recent years; these devices may now be opened using the owner's fingerprint data. These biometric systems are becoming more and more common due in large part to their capacity to discern between a legitimate user and a dishonest one.

Since fingerprint biometrics are easier to use and less expensive to maintain than other mechanisms, it is now believed that they are the most often used technique. However, security and confidentiality are issues that must be disregarded as these apps continue to grow in development. According to Kindt (2016), many of the advantages of biometrics can quickly turn into disadvantages, maintaining the security and integrity of biometric data is a significant concern. Therefore, it becomes imperative to protect biometric data, especially fingerprint data, in order to encourage the widespread use of biometric technology.

The fingerprints biometrics are nothing but images which are very much economical to store compared to other methods. Because biometric information is frequently used as verification for government identity cards, it is vulnerable to attack and might be used by hackers to steal money. So there is a need of securing these fingerprint data which is stored as image. Providing security means we need to encrypt the fingerprints and store so that the attackers could not recognize the pattern and thus will be refrained from causing any financial loss. In encryption, the image we encrypt is referred to as the "plain image," and the "cipher image" is the name of the encrypted image.

Belazi *et al.* (2016) mentioned that when it comes to security, complexity, speed, processing power, computational overhead, and other crucial aspects, chaos-based encryption algorithms stand out for having a number of really positive features. According to Shahna *et al.* (2020), owing to inherent characteristics of images, notably their substantial storage capacity and robust pixel correlation, conventional encryption methods like DES, IDEA, and RSA are not suitable for realistic image encryption, particularly when used in the context of online communications.

Because of the intrinsic qualities of images, such as more redundancy and capacity for large amounts of data, which are typically challenging to manage by conventional approaches, image data encryption differs from that of text data as mentioned by Essaid *et al.* (2018). Hosny *et al.* (2022) proposed a novel and effective solution to the intractable challenge of quick as well as extremely safe image encryption due to the unusually desired qualities of mixing and susceptibility to chaotic map parameters and preliminary conditions. A proper chaos-based cryptosystem consists of an encryption technique that has good prospects for securing image data by confusing and diffusing the image pixels as declared by Li *et al.* (2017).

Wang *et al.* (2019) and Ye (2010) said that chaotic theory is gaining large attention in image encryption field due to its exceptional performance, high sensitivity to initial metrics, unexpected nature, ergodicity of states, plus additional elements. Any chaotic system goes through two stages: confusion and diffusion. Confusion is intended to make it more challenging to understand the connection between the cipher image and the key.

Whereas, diffusion aims to achieve maximum complexity in the link amid the cipher image and the plain image. It does, however, make a simple image more secure for transmission at the expense

of increased computation time complexity. Thus to keep balance between the two, we have created a fingerprint image encryption system based on dual confusion where we have divided and rotated image pixels and applied a pixel shifting algorithm to the resultant image followed by a diffusion process.

This is how the rest of the document is structured. Some financial aspects of biometrics are discussed in Section 2. We have reviewed some recent related research studies in Section 3. A detailed explanation of the proposed system is provided in Section 4. The experiment carried out to support the suggested network's performance is detailed in Section 5, Section 6 presents the findings and the conclusion in summarized in Section 7.

Financial aspects of Biometrics

When biometrics are mentioned, images of face scanning in crowds and fingerprint dusting instantly come to mind. Of course, facial and fingerprint identification are two of the best instances of biometric technology in action. A biometric system consists of several components. A biometric sensor receives a user's biometric feature, records it, and outputs a measured signal. The user's biometric may be altered during the measurement by a number of noise factors, including differences in user involvement, ambient changes, and sensor constraints. Feature extraction converts the measured signal into a biometric template, a condensed yet expressive representation of the biometric characteristic after the sensor records the trait.

A biometric system consists of two distinct stages. During the enrollment step, the user's biometric trait is obtained by the biometric system, which then extracts the template and stores it in a database along with an identification that connects the template to the user's identity. The biometric system gathers the user's biometric trait, extracts the template, and compares it with the template(s) in the database during the second step of recognition. Fig. 1 shows biometric system.

With the adoption of new technologies and the accompanying changes in user behavior, the financial services sector has undergone significant changes in recent years. The growth of potent computer devices, such as mobile phones, laptops and tablets has altered how people engage with financial services (banks, e-commerce sites, etc.).

One of the industries that has adopted biometric technologies the quickest is financial services. These technologies have advantages in many different fields. This can be mostly attributed to the recent wave of digitization that has raced through the industry. Financial services companies are realizing the need for stronger authentication security than what is offered by password-based systems as more and more customers do their banking online.

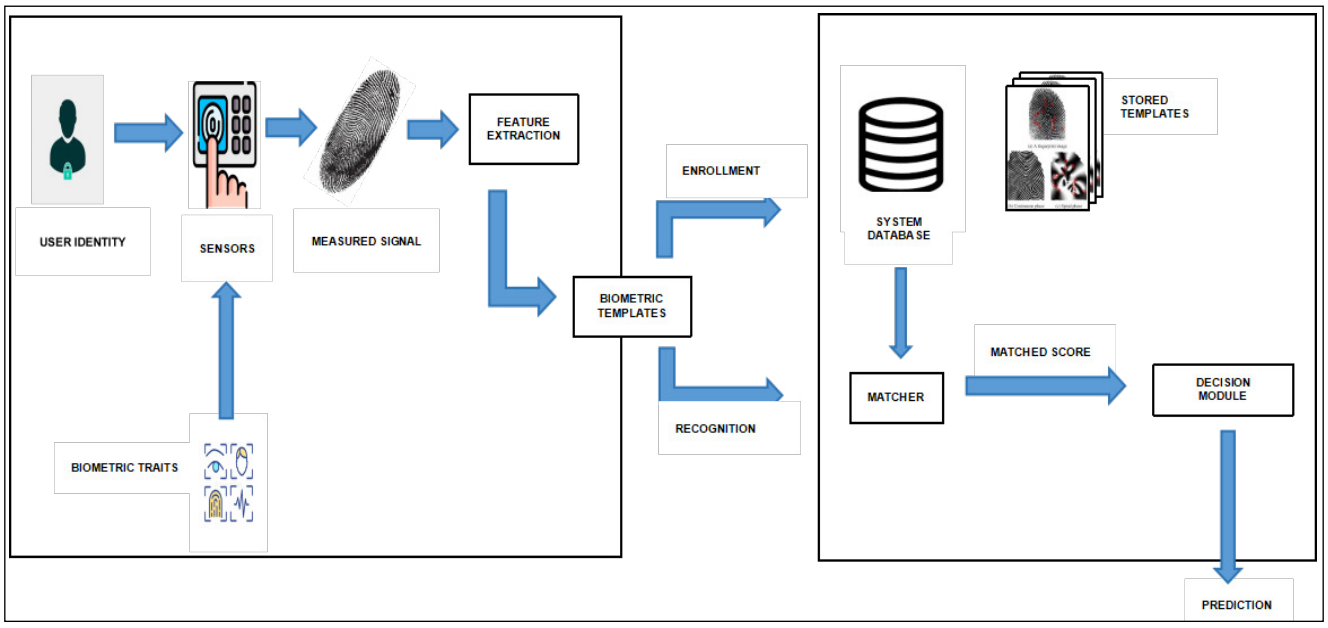

Fig. 1: Biometric system

But there is no guarantee that a biometric system will be totally safe, even though the primary reason for using one is to shield an application from unwanted access. Similar to other security systems, the biometric system is susceptible to several security risks. These threats could potentially compromise the financial and economic security of the final application. Adverse outcomes include financial forgery, denial-of-service attacks against authorized users, unauthorized user intrusions, corrupt users' repudiation claims, and function creep-related erosion of user privacy could result from these security flaws. Numerous research have thoroughly examined the security risks that biometric systems confront and have recommended countermeasures.

So, in our case also we have developed a financially secure cryptosystem so that no financial forgery can happen with our fingerprint data that are used nowadays in various official works.

Related work

Some of the most recent cutting-edge methods were followed for studying chaotic systems in this section. As discussed in the previous section, chaotic systems are based on proper confusion and diffusion.

For color images, Sridevi *et al.* (2022) have developed an encryption method based on double confusion and double diffusion. The color pictures' RGB planes are separated. Duo diffusion and duo confusion have been used to achieve the encryption on RGB planes using chaotic maps and attractors. Different initial conditions and seeds have been utilized to execute confusion and diffusion in each plane in two stages, namely, block and plane, using the Logistic Map, Lorenz Attractor, Tent Map, and Lu Attractor. An encrypted image has been created by combining the split RGB planes.

A coupling chaotic system was presented by Hu and Li (2021) that can merge any two one dimensional chaotic maps to create a new one that performs better in applications related to cryptography. A particular unit transform is the foundation of the coupled chaotic system. To further increase the randomness of chaotic sequences, a pseudo-random number generator based on chaos is developed. Additionally, they have developed a technique where the higher and lower bits of the input images will be encrypted independently using a two-way multi-round transformation network.

A method of encrypting color images using chaotic transform orders and a real fractional Hartley transform has been devised by Kaur *et al.* (2022) Both piecewise linear and piecewise non-linear chaotic maps make up the multilayer system. The chaotic map's input parameters act as a secret key. A list of fractional Meixner polynomials together with an explanation of their properties and a thorough method for obtaining them were proposed by Karmouni *et al.* (2021) They presented FrDMM-based encryption and decryption techniques for both color and grayscale images.

Multiple chaotic maps are the basis for the image cryptosystem and they have properties like ergodicity and sensitivity to control parameters and beginning conditions. The process of creating a shuffled image involves randomly arranging its pixels. It is then dispersed by XORing its pixels using a private key. Several chaotic maps are combined to create this key. Elkandoz *et al.* (2022) presented an image encryption technique that entails Arnold map to first jumble the image's pixels. Second, a two dimensional Logistic Sine map and a congruential generator are used to create a 256-bit key. Then, using the key to XOR the shuffled image's pixel values, the encrypted image is produced.

An image block encryption technique based on several chaotic maps has been suggested by Ma *et al.* (2020) Certain plain images can be used to readily extract its equivalent secret key. A function known as Generating function for typical period-doubling to chaotic Chebyshev polynomials was presented by Louzzani *et al.* (2021). They utilized the bifurcation diagram and the Lyapunov exponent and developed a generating function which is a deterministic system with chaotic behavior. Sekar *et al.* (2022) developed a novel image encryption method by utilizing chaotic encryption theory and diagonal shuffling. The suggested approach includes two-dimensional Henon, Ikeda chaotic maps, and shuffling algorithms. A random image pixel is substituted after a random S-Box that has been generated using Henon Map has been chosen.

Haddada *et al.* (2017) proposed a novel approach to watermarking reinforcement that preserves reduced

storage space and a high quality of watermarked host image while guaranteeing an appropriate trade-off between the computational complexity of the proposed scheme and the security level of an individual's biometric data.

In this study, we have proposed divide-rotate and pixel shifting based chaotic cryptosystem. As was previously said, a cryptosystem with chaotic elements produces a lot of confusion and diffusion, which improves security. Thus, we have developed an image cryptosystem that outperforms existing cutting-edge techniques and is extremely safe.

Proposed image cryptosystem

Our proposed image cryptosystem is discussed in this section. A chaotic image cryptosystem is designed to develop a cipher image based on dual confusion carried by a diffusion process. Divide-rotate algorithm and pixel shifting algorithm are designed to perform the dual confusion process in this proposed scheme. The diffusion process is executed with the assistance of pseudo-random sequence generator developed using Logistic map. Fig. 2 represents the block diagram of our proposed scheme.

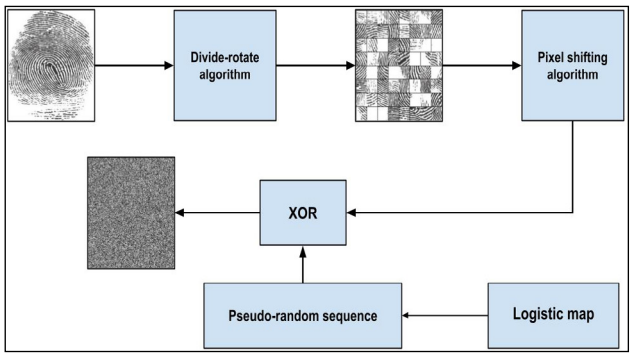

Fig. 2: Block diagram of the proposed image encryption scheme

Divide-rotate Algorithm

We have designed a divide-rotate algorithm for the 1st round of confusion process which is basically used to shuffle the image so that we can create more degree of unpredictability in the encrypted image. The new technique has been described with an algorithm given in Algorithm 1.

Algorithm 1: Divide-rotate algorithm

1. Set Size = 64 to generate a random sequence using Logistic map.
2. Store the random sequence in vv[ ].
3. Divide the image into 64 equal parts and name them as numbers ranging from 0 to 63.
4. Rotate the image parts into 90 degrees and 180 degrees alternately i.e. odd parts by 180 degrees and even parts by 90 degrees as described in Fig. 3.
5. Initialize 8 empty vectors b0, b1, b2, b3, b4, b5, b6, b7.
6. Now store all the values from vv to the vectors b0, b1, b2, b3, b4, b5, b6, b7 where each vector contains 8 values.
7. Set Size = 8 to generate a random sequence using Logistic map.
8. Set index_values = [64, 65, 66, 67, 68, 69, 70, 71].
9. Store the random sequence in vv1[ ].
10. Change the index_values to array.
11. Rearrange the index_values as per the sequence of the values of vv1.
12. Now join the divided image parts horizontally as per the values in the vectors b0, b1, b2, b3, b4, b5, b6, b7 as elaborated in Fig. 4.
13. Then name the horizontally joined image as numbers ranging from 64 to 71.
14. Now join the horizontally joined image parts vertically as per the sequence in vv1 and name as v image.

The working procedure of the algorithm is elaborated with the help of the diagram given in Fig. 2.

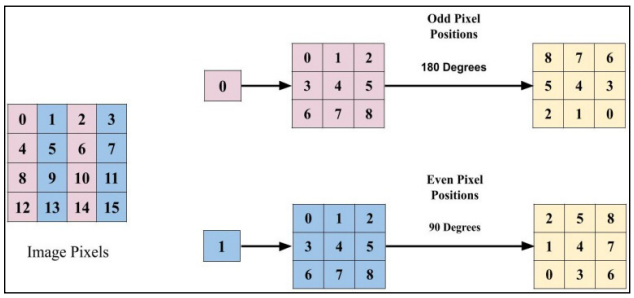

Fig. 3: Working of Diivide-rotate algorith Pixel shifting algorithm

For performing the 2nd round of confusion, we have designed a pixel shifting algorithm. In this algorithm we have rearranged the pixels in clockwise and anti-clockwise as shown in Fig 3.

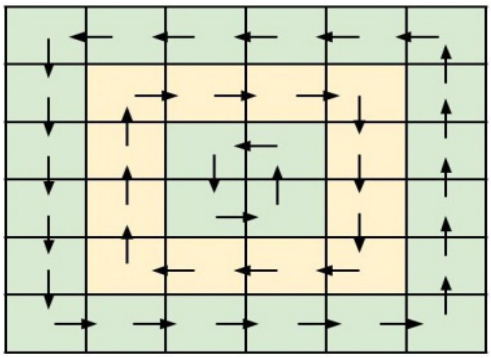

Fig. 4: Working of pixel shifting algorithm

Pseudo-random sequence generator

In the diffusion process, we have generated a pseudo-random sequence of 256 × 256 number of values using the Logistic map so that we can perform an XOR operation with the confused image. Algorithm 2 provides the pseudo-random sequence generation algorithm.

Algorithm 2: Pseudo-random sequence generation Algorithm

1. Generate primary value $x_0 \in (0,1)$ and control metric values r ∈ (0,4) from the chaotic range.
2. Set $x_{old} = x_0$.
3. Calculate the height and width of the image.
4. Set limit = height of the image × width of the image.
5. Initialize a empty vector ran_num.
6. for i in range(limit)
7. $x_{new} \leftarrow r \times x_{old} \times (1 - x_{old})$
8. ran_num $\leftarrow (abs(x_{new} \times 107)) \bmod 256$
9. end for
10. return ran_num.

Image encryption steps

The steps to design the proposed scheme are discussed in the following algorithm:

Algorithm 3: Encryption Algorithm

1. Import an image P of size M × N.
2. Apply the Divide-rotate algorithm (Ref. **Algorithm 1**).
3. img = img1.
4. Apply the pixel shifting algorithm.
5. img = img2.
6. Apply the pseudo-random sequence (Ref. **Algorithm 2**) to generate M × N number of random sequence $R1$.
7. The name of the generated image from the above step is P1 .
8. Set Size= M × N.
9. for i in range(Size):
10. P2[i] ← XOR(P1[i], $R1$[i])]
11. end for
12. The P2 image is considered as cipher image C of size M × N.

Image decryption steps

Decryption is the reverse concept of the encryption process. Inverse diffusion should be done to get the confused image and then the confused steps need to be inversed to get the original image.

Performance and Security Analysis

The proposed scheme is analyzed with the help of some fingerprint images taken from test database. The following analysis have been performed to examine the proposed cryptosystem's performance and security strength.

Entropy analysis

The degree of randomness in an encrypted image is examined using entropy. A more random image is considered to be more secure. The values of entropy that correspond to the highest and lowest degree of randomness in an image are 8 and 0, respectively.

The fingerprint we took for analysis i.e., the plain image has entropy value 6.4011. After analysis, we found that after applying our proposed scheme over the plain image, we got the entropy value as 7.9987 for the cipher image. So, it is clear from that our proposed scheme has high degree of randomness and can resist entropy based attack.

Statistical attack analysis

The statistical analysis describes how the plain and cipher images are related. There are two varieties of statistical analysis: Histogram and Correlation analysis. They are mentioned below:

(a) Histogram analysis

A histogram displays the pixel distributions in an image to gauge how well an encryption technique works. The histogram of a cipher image in a suitable encryption method should be uniformly flat. Fig. 5 displays both the encryption image histogram and the plain image fingerprint histogram that were used to examine our suggested strategy. The pixel intensities in Fig. 5 are consistently distributed, making them resistant to statistical attack.

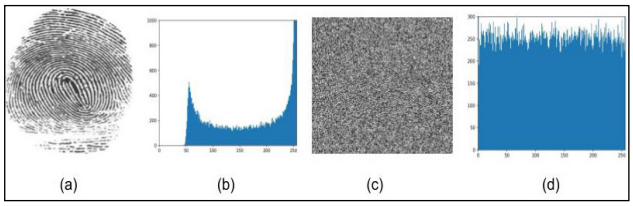

Fig. 5: Histogram analysis of fingerprint plain image and its corresponding cipher image

(b) Correlation analysis

The extent to which adjacent pixels in an image are correlated is measured by correlation. In essence, there is a high association between adjacent pixels in a plain image. However, the cipher image in a sound cryptosystem should have little correlation. In general, the encrypted image's value is close to 0, and the plain image's correlation coefficient value is close to 1, or high. It is evident from Table 1 that the correlation between neighboring pixels is completely disrupted by our suggested encryption method. As a result, the suggested plan is immune to statistical attacks.

Table 1: Correlation Coefficient values of plain and cipher images

Plain image (fingerprint)			Cipher image		
Horizontal	*Vertical*	*Diagonal*	*Horizontal*	*Vertical*	*Diagonal*
0.9436	0.9635	0.9268	0.0046	-0.0018	0.0126

Key space analysis

Ideally, the entire key search space will be larger than 2^{100} to prevent brute-force attacks. The pseudo-random sequence in this study is generated using the Logistic map.

Two parameters on the Logistic map, x and r, are employed as a secret key during the encryption procedure. Because of this, our experiment's overall key search space is $10^{64} \approx 2^{213}$, with a computational accuracy limit of 10^{-16}.

Differential attack analysis

The values of UACI (unified average changing intensity) and NPCR (number of pixel change rate) are assessed in order to assess the security of the suggested encryption system against differential assaults. For NPCR and UACI, the optimal values are approximately 99% and 33%, respectively. For our proposed system, the NPCR value is 99.65 and the UACI value is 33.57. So, our proposed system is near to the ideal value and thus can resist differential attack.

Execution speed

The executions are conducted by Python 3.8.0 in HP Laptop with Intel(R) Core(TM) i5-8250U CPU @ 1.80 GHz, 8GB RAM. The encryption time required for encrypting the fingerprint plain image is 0.2534 seconds. Thus the proposed scheme can handle a large volume of data in less time.

Comparative Analysis

The proposed scheme was compared with respect to correlation coefficient values, entropy values, NPCR and UACI metrics. The comparison was made with various state-of-the-art schemes based on fingerprint images. It was found that the proposed scheme has a high entropy value than the other existing techniques, and the correlation values are close to 0, indicating that the adjacency between each pixel after encryption is less. Moreover, the NPCR and UACI values refer to the optimal values for our suggested system and the execution speed is also less compared to the other existing schemes.

CONCLUSION

This paper has presented a chaotic biometric cryptosystem with fingerprint data by designing a divide-rotate algorithm and pixel shifting algorithm. A secure encryption technique should have a good amount of confusion and diffusion, and the proposed method has this property to a large extent. Further, pseudo-random sequence generator based on Logistic map is applied in the diffusion process for better encryption effect. The result of histogram analysis and correlation analysis shows that the

proposed scheme is resistant to statistical attacks. Additionally, there is a lot of randomness in the suggested plan and thus can resist entropy based attacks. The proposed method can also resist brute-force attacks and differential attacks and thus is suitable for real-time applications. Also comparing with the all existing schemes, it has been found that our suggested system yields greater results. Thus our proposed scheme can resist various attacks and thus can reduce financial loss. Also fingerprint data are economical to store and by the use of this scheme, financial security measures has also increased with time efficiency.

REFERENCES

Belazi, A., Abd El-Latif, A.A. and Belghith, S. 2016. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing,* **128**: 155-170.

Dunstone, T. and Yager, N. (Eds.). 2009. Biometric system and data analysis: Design, evaluation, and data mining. *Boston, MA: Springer US*.

Elkandoz, M.T. and Alexan, W. 2022. Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications,* **81**(18): 25497-25518.

Essaid, M., Akharraz, I., Saaidi, A. and Mouhib, A. 2018. A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. *Procedia Computer Science*, **127**: 539-548.

Haddada, Lamia Rzouga, Bernadette Dorizzi, and Najoua Essoukri Ben Amara. 2017. Combined watermarking approach for securing biometric data." *Signal Processing: Image Communication,* **55**: 23-31.

Hosny, K.M., Kamal, S.T. and Darwish, M.M. 2022. A color image encryption technique using block scrambling and chaos. *Multimedia Tools and Applications,* pp. 1-21.

Hu, G. and Li, B. 2021. Coupling chaotic system based on unit transform and its applications in image encryption. *Signal Processing,* **178**: 107790.

Karmouni, H., Sayyouri, M. and Qjidaa, H. 2021. A novel image encryption method based on fractional discrete Meixner moments. *Optics and Lasers in Engineering,* **137**: 106346.

Kaur, G., Agarwal, R. and Patidar, V. 2022. Color image encryption system using combination of robust chaos and chaotic order fractional Hartley transformation. *Journal of King Saud University-Computer and Information Sciences,* **34**(8): 5883-5897.

Kindt, E.J. 2016. Privacy and data protection issues of biometric applications (Vol. 1). *New York: Springer.*

Li, C., Lin, D. and Lü, J. 2017. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multi Media,* **24**(3): 64-71.

Louzzani, N., Boukabou, A., Bahi, H. and Boussayoud, A. 2021. A novel chaos based generating function of the Chebyshev polynomials and its applications in image encryption. *Chaos, Solitons & Fractals,* **151**: 111315.

Ma, Y., Li, C. and Ou, B. 2020. Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications,* **54**: 102566.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G. and Yearwood, J. 2016. Protection of privacy in biometric data. *IEEE Access,* **4**: 880-892.

Sekar, J.G., Arun, C., Abilash, V.M., Aravindan, K., Barathiselvan, K. and Bharath, J. 2022. A modified chaotic image encryption scheme for color image using diagonal pixel confusion and diffusion method. *In AIP Conference Proceedings* (Vol. 2405, No. 1). AIP Publishing.

Shahna, K.U. and Mohamed, A. 2020. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. *Applied Soft Computing,* **90**: 106162.

Sridevi, A., Sivaraman, R., Balasubramaniam, V., Sreenithi, Siva, J., Thanikaiselvan, V. and Rengarajan, A. 2022. On Chaos based duo confusion duo diffusion for colour images. *Multimedia Tools and Applications,* **81**(12): 16987-17014.

Wang, X.Y. and Li, Z.M. 2019. A color image encryption algorithm based on Hopfield chaotic neural network. *Optics and Lasers in Engineering,* **115**: 107-118.

Ye, G. 2010. Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters,* **31**(5): 347-354.