Lossless Encryption Technique for Finger Biometric Images

Pranoti G. Tapase[1], Prof. G. N. Wazurkar[2], Dr. D. R. Dandekar[3]

[1]PG Scholar, Department of Electronics Engineering, BDCE, Sevagram, Wardha –442102, INDIA
[2]Assistant Professor, Department of Electronics Engineering, BDCE, Sevagram, Wardha –442102, INDIA
[3]Professor, Department of Electronics Engineering, BDCE, Sevagram, Wardha –442102, INDIA

---***---

Abstract - *Biometric template protection is one of the most important issues in deploying a practical biometric system. To tackle this problem, many algorithms, that do not store the template in its original form, have been reported in recent years. They can be categorized into two approaches, namely biometric cryptosystem and transform-based. However, most algorithms in both approaches offer a trade-off between the template security and matching performance. Moreover, it is believed that no single template protection method is capable of satisfying the security and performance simultaneously. Multi-biometric systems are being increasingly deployed in many large-scale biometric applications (e.g., FBI-IAFIS, UIDAI system in India) because of their advantages of lower error rates and larger population coverage compared to uni-biometric systems. However, multi-biometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security.*

Keywords: encryption algorithm, decryption algorithm, attacks.

1. INTRODUCTION

With the growth in communication technology, the popularity of multimedia data has also increased. The progress in multimedia distribution technology has resulted in easy availability of multimedia content to various users over the communication channels. Users of the multimedia data are able to carry out real-time audio and video conferencing, listen to music, view streaming video clips, etc. They also view films and news on the World Wide Web (WWW). However, most of the networks used for multimedia distribution are open channels and are highly insecure. These networks are vulnerable to attacks and not suitable for transmitting sensitive and valuable multimedia content such as military, financial or personal videos. This necessitates secure encryption algorithms for multimedia data protection. Cryptography is an important tool in modern electronic security technologies to protect valuable multimedia data on intranets, extranets and the Internet. Data encryption is encoding the data so that only authorized users can decode the content. For all others, the data does not make any sense. Encryption algorithms have been well studied for the textual data in the past. This standard has resulted in algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), RC4, RC6, etc. However, direct extension of the algorithms for image does not result in practically useful image encryption schemes. All these algorithms are designed based on the textual characteristics. Image encryption schemes are different from textual encryption because image data are usually large in size and thus requires more time for encryption. It also requires a similar amount of time for decryption. Computational overhead makes the traditional encryption algorithm unsuitable for real-time image communications.

2. LITERATURE REVIEW

Image Security ensures protection of image content using classical encryption algorithms. Figure 1 shows the general block diagram of encryption/decryption system. The original content is changed into the encrypted form with the encryption algorithm using encryption key. In the same way the encrypted data is decrypted into the original format with the decryption algorithm using the same key.

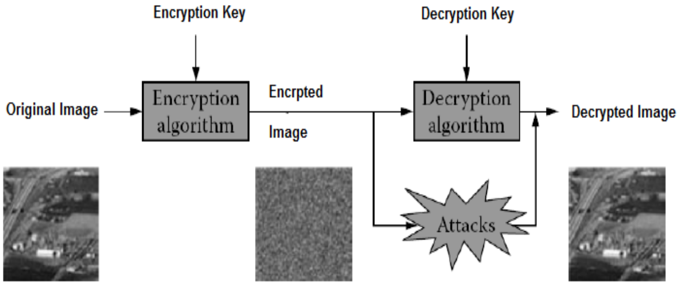

Fig. 1. Image Encryption & Decryption System

Requirement for image encryption/decryption

- Security: Security is the essential requirement of image content encryption and it can be viewed in two aspects namely cryptographic security and perceptual security. The cryptographic security mainly deals with cryptographic attacks and perceptual security makes the image content garbled to human insight. The encryption algorithm becomes secure if the cost of breaking is more than content. The cryptographic security is the ability to resist the attacks like differential attack, cipher-text only attack, plain-text only attack and statistical attack. If any new formulated algorithm is secure against those attacks, the encryption algorithm is said to be of high security, otherwise regarded as of low security.

- Compression: In general image data is compressed to minimize the storage space or transmission bandwidth. The image content may be encrypted before compression, during compression and after compression based on its applications. Due to encryption algorithms, the size of image content may increase than the original data.

- Encryption efficiency: Most of the encryption algorithms are required for real time applications therefore they should be more efficient and allow less delay during transmission through the network or at the time of user access. This can be achieved by reducing encrypted data volume and proposing light weight algorithms.

Encryption can be classified into two types

1. Complete Encryption: Complete encryption encrypts the entire image content without considering its format. This kind of algorithm encrypts raw data or compressed data directly with classical encryption algorithms by using an encryption key. In raw data encryption, the image data is encrypted before it is compressed. In compressed data encryption, the data is first compressed and then encrypted. Based on the properties, encryption algorithms can be classified into permutation algorithms, random modulation algorithms, confusion diffusion algorithms, and partial DES algorithms, etc. Based on implementation, they can be classified into software based algorithms and hardware-based algorithms.

2. Selective Encryption: Selective encryption approach encrypts only a part of the image content. Image data is first partitioned into two parts, one part is encrypted by encryption algorithm with encryption key, and the other part is not changed, and the two parts are combined together. The decryption process is symmetric to the encryption process.

Applications of image encryption / decryption

- Internet communication
- Medical imaging
- Military communication
- Cryptography
- Steganography
- Digital image watermarking
- Biometric images

[1] In this paper two stage biometric data protection scheme is being proposed using permutation and substitution mechanism of the chaotic theory which is lossless in nature. Arnold transformation and Henon map is used to design an efficient encryption system. The encryption method is aimed at generating an encrypted image that will have statistical properties completely dissimilar from the original image analysis which will make it difficult for any intruder to decrypt the image. The performance of the method has been experimentally analyzed using statistical analysis and correlation based methods. Correlation coefficient analysis is done to evaluate the behavior of pixels in horizontal and vertical directions and the results are found to be encouraging. This protection scheme provides the ability to encrypt the data and secure it from unauthorized users. Upon decryption the data is completely recovered making this scheme a lossless and efficient method of biometric data security.

[2] Biometric identification suffers a lot of problems such as the storage of user's biometric template, the leakage of user's private and the resulting security problems. As a substitution, biometric encryption has become the focus of the present studies. Recently, numerous studies focus on biometric encryption based on Fuzzy Vault, Fuzzy Commitment and dynamic key generation. Both of them are unavailable in the network environment as they suffer neither stored templates nor unstable keys. In this paper, we propose a fingerprint encryption scheme based on threshold (t, n), unlike the reliance of templates in Fuzzy Vault based scheme or the "encrypted" templates in Fuzzy Commitment based scheme when regenerate the very key, which protects biometric key in a polynomial, and saves nothing about biometric characteristics just like dynamic biometric key generation scheme.

[3] With the current emergence of biometric image data applications on devices such as smart phones, security cameras, personal computers etc, there is a need for securing the image templates obtained from crime scenes as well as such devices before storing them in locations such as the cloud etc. In this paper, we proposed an encryption technique of securing the biometric image data collected from devices with an approach of feature based on encryption technique for securing forensic biometric image data using AES and visual cryptography method.

[4] In this paper, a chaotic encryption framework is proposed for enhancing the security of biometrics images during transmission. The proposed framework is based on the fractional wavelet packet transform (FrWPT), chaotic map and Hessenberg decomposition. The core idea is to shuffle biometrics image using affine transform followed by the transformation in FrWPT domain with chaotically generated transform orders. Now, FrWPT coefficients are altered using the Hessenberg decomposition. Finally, a reliable decryption process is presented to reconstruct original biometrics image from the encrypted data only with the valid keys. The efficiency and robustness of the proposed technique are validated by different kind of simulations and analysis on fingerprint images.

[5] This study proposes a chaos-based image encryption scheme using Henon map and Lorenz equation with multiple levels of diffusion. The Henon map is used for confusion and the Lorenz equation for diffusion. Apart from the Lorenz equation, another matrix with the same size as the original image is generated which is a complex function of the original image. This matrix which is configured as a diffusion

matrix permits two stages of diffusion. Due to this step, there is a strong sensitivity to input image. This encryption algorithm has high key space, entropy very close to eight (for grey images) and very less correlation among adjacent pixels. The highlight of this method is the ideal number of pixels change rate and unified average changing intensity it offers. These ideal values indicate that the encrypted images produced by this proposed scheme are random-like. Further, a cryptanalysis study has been carried out to prove that the proposed algorithm is resistant to known attacks.

3. PROBLEM FORMULATION

The objective of our research is to develop and investigate the performance of encryption / decryption algorithm for finger biometric images using cryptosystem technique by measuring encryption time, NPCR, UACI and entropy.

- To develop encryption algorithm
- To develop decryption algorithm
- Performance evaluation using parameters under common attacks such as noise, geometric and compression.

4. PROPOSED METHODOLOGY

The following steps indicate the methodology adopted for biometric image encryption/decryption.

1. Input fingerprint biometric image
2. Preprocessing of input image
3. Key generation
4. Encryption / decryption algorithm
5. Key management
6. Performance evaluation using parameters under common attacks such as noise, geometric and compression.

5. CONCLUSION

Two important attributes of a powerful encryption technique are diffusion and confusion. Hence, the motivation is to generate a scheme which has more diffusion and confusion. Due to some intrinsic features of images, some of the traditional encryption schemes are not very suitable for finger biometric images encryption. Hence the motivation is to generate schemes to encrypt images efficiently. To enhance the security of images, a biometric cryptosystem approach that combines cryptography and biometrics images. Under this approach, the biometric image is encrypted with the help of key. A key may be generated with the combination of fingerprint image itself and / or password and is used for image encryption. This mechanism is seen to enhance the security of biometrics images during transmission, storage and verification

ACKNOWLEDGEMENT

Firstly, I would like to thank respected Dr. D. R. Dandekar sir and Prof. G. N. Wazurkar sir for giving me such a wonderful opportunity to expand my knowledge and for his huge support. Secondly, I would like to thank my parents who patiently helped me as I went through my work and my friends who helped me to make my work more organized and well-stacked till the end.

REFERENCES

[1] Garima Mehta, Malay Kishore Dutta, Jan Karasek, Pyung Soo Kim, “An Efficient and Lossless Fingerprint Encryption Algorithm Using Henon Map & Arnold Transformation,” in IEEE International Conference on Control Communication and Computing (ICCC), 2013.

[2] Bin Liang, et al, “A Novel Fingerprint-Based Biometric Encryption,” in IEEE Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2014.

[3] Quist-Aphetsi Kester, et al, “Feature Based Encryption Technique For Securing Forensic Biometric Image Data Using AES and Visual Cryptography,” in IEEE Second International Conference on Artificial Intelligence, Modelling and Simulation, 2014.

[4] G. Bhatnagar and Q. J. Wu, “Enhancing the transmission security of biometric images using chaotic encryption,” Springer Multimedia systems, vol. 20, no. 2, pp. 203–214, 2014.

[5] Brindha Murugan, Ammasai Gounden Nanjappa Gounder, “Image encryption scheme based on block based confusion and multiple levels of diffusion,” in IET Computer Vision, Vol. 10 Issue 6, 2016, pp. 593-602.

[6] R. Gonzales, R. E. Woods, “Digital Image Processing,” 2nd Edition, New Jersey Prentice Hall, 2002.

[7] A. K. Jain, “Fundamentals of Digital Image Processing,” 2nd Edition, Prentice Hall, 1994.