IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 1, January 2018

Securing Digital Data using 256-bit Multimodal Biometrics based Cryptographic Key

Pooja Muthamma M.M[1], Lakshmisha S Krishna[2]

PG Student, VLSI Design & Embedded Systems, Alpha College of Engg, Bengaluru, India[1]

Assistant Professor, Dept of Electronics & Communication Engg, Alpha College of Engg, Bengaluru, India[2]

Abstract: In the current era of digitisation, digital documents are widely used. The merits of digital documents are huge while its security and privacy are at large. Hence Cryptography is used to secure digital documents. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. In this paper a novel idea is proposed, digital documents are encrypted using 256- bit cryptographic key which is generated by multimodal biometric system. This system uses Palm print and Fingerprint as traits. The features of both traits were extracted and fused at feature level. This biometric based cryptographic key is unpredictable to an intruder as the intruder lacks the knowledge of physical traits of the user. By this proposed model confidentiality, integrity, availability mechanisms are achieved. This biometric based cryptographic security can be integrated to e-governance and e-health for efficient management.

Keywords: Securing digital documents, to stop fraudulent activities, palm print, fingerprint, Impossible to forge, Impossible to counterfeit secured data, multimodal biometric system, cryptographic security, e-governance, e-health

I. INTRODUCTION

The multimodal biometric systems has played a prominent role in many of present days applications ranging from healthcare industries, military to many of commercial applications such as airports and bank industries. The implication towards the rising demand for more robust, efficient and secure identification systems has caused the development of many advanced methods for realizing the above criteria. Various analysts have contemplated the communication amongst biometrics and cryptography, two possibly integral security innovations. Biometrics is about measuring one of a kind individual components, for example, a subject's voice, unique mark, or iris. It can possibly distinguish people with a high level of confirmation, along these lines giving an establishment to trust. Cryptography, then again, frets about the projection of trust: with taking trust from where it exists to where it is required. A solid mix of biometrics and cryptography may, for instance, can possibly connect a client with a computerized signature she made with an abnormal state of affirmation. For instance, it will end up noticeably harder to utilize a stolen token to produce a mark or for a client to dishonestly renounce a mark by guaranteeing that the token was stolen when it was definitely not. Past endeavours toward this path incorporate a signature verification pen and related flag processor made accessible with the IBM Transaction Security System in 1989.

One issue with this approach is its total dependence on equipment alter resistance: If the token is broken, both the layout and the key are lost. Much of the time, assailants have possessed the capacity to break tokens, regardless of whether by equipment assaults abusing chip-testing innovation or (as with the IBM plan) by API assaults on the token's product. We subsequently embarked to locate a superior method for joining biometrics, cryptography, and alter resistance. The principle snag to algorithmic blend is that biometric information are loud; just a surmised match can be relied upon to a put away format. Cryptography, then again, requires that keys be precisely right, or conventions will come up short. Thus, past item offerings have been founded on particular equipment gadgets. It is ideal to have a more broad, convention level approach, joining cryptography and biometrics. However another thought is protection. Numerous clients might be hesitant to have biometric information put away on focal databases; there might be less imperviousness to biometric innovation if clients can be believably guaranteed that their layouts are not put away midway (or, maybe, by any stretch of the imagination). Different specialists have attempted to delineate information into a remarkable and repeatable twofold string.

Along these lines, the paired string would be mapped to an encryption key by alluding to a query table or coordinate hashing. The capability of this approach is that capacity of a biometric layout would not be required. Up until now, nonetheless, these endeavours have experienced a few disadvantages, which we will now clarify. In the paper, we will utilize the term biometric key, proposed in, to allude to the repeatable string gotten from a client biometric. The most difficult issue with biometrics is the lack of quality of individual bits in the format. Biometric estimations, being made of traits of the human body, are loud by nature, while cryptography requests rightness in keys.

DOI 10.17148/IJARCCE.2018.713

There have been many endeavours to cross over any barrier between the fluffiness of biometrics and the exactitude of cryptography by getting biometric keys from keystroke designs, the human voice, manually written marks, fingerprints, and facial attributes. Be that as it may, up until this point, these endeavours have experienced an exorbitant False Rejection Rate (FRR) normally more than 20 percent, which is unsatisfactory for down to earth applications. Second, numerous recommendations have neglected to consider security building perspectives, of which the most serious are the permanence of biometrics and their low level of mystery. Biometric highlights are intrinsic in people, so they can't be changed effortlessly. A related issue is key assorted qualities: A client may wish isolate keys for her financial balance and for access to her working environment PC so she can renounce one without influencing the other. Third, biometric information are not extremely mystery. Individuals leave (low quality) fingerprints all over and iris pictures might be caught by a concealed camera. As a rule, the more a biometric is utilized, the less mystery it will be. It is impulsive to depend on a biometric alone, particularly if that biometric wound up noticeably utilized on a worldwide scale (for instance, in the biometric character cards proposed in a few nations). Fourth, social acknowledgment is significantly essential to the accomplishment of biometric innovation. The dread of the potential abuse of biometric information may make people in general hesitant to utilize frameworks that rely upon it and this could be particularly the case if there is a huge focal database of biometric information which centers protection stresses and goes about as an objective of security activists. There might be a dread that individual wellbeing data will spill out by means of biometric information and there may even be religious protests.

A. Image Encryption And Decryption

The recent advancements in the field of Digital multimedia have created a demand with respect to security of the data. Applications such as Pay-Tv, remote video conferencing, and medical imaging demand a secure data which leads to the development of encryption algorithms. Many encryption algorithms has been proposed and developed over the last four decades leading to creating standards pertaining to encryption. Some of the noted and accepted standards over the world include *Data Encryption Standard* (DES) initially created by

IBM on public request, another such standard pertaining to encryption is the *Advanced Encryption Standard* (AES). The basic block diagram for DES is given in fig 1.1. The digital images have a grid like structure which basically involves two operations while performing encryption. They are

1) *Position permutations*: This operation is the most commonly used operation in image encryption. The permutations applicable to both spacial and frequency domains. Its main advantage lies in its easy implementations. permutation dissipates the statistical structure of the plaintext into long range statistics and it is suitable for fast processing requirements of massive digital multimedia data

2) *Value Transformation*: This operation performs transformation on the image pixel values. Some times in order to obtain a high secured data, the position permutation and a simple value transformation such as XOR operation are performed. Such type of operations involving both the methods could be called as *combinational operation*.

Data Encryption structure (DES) general block diagram

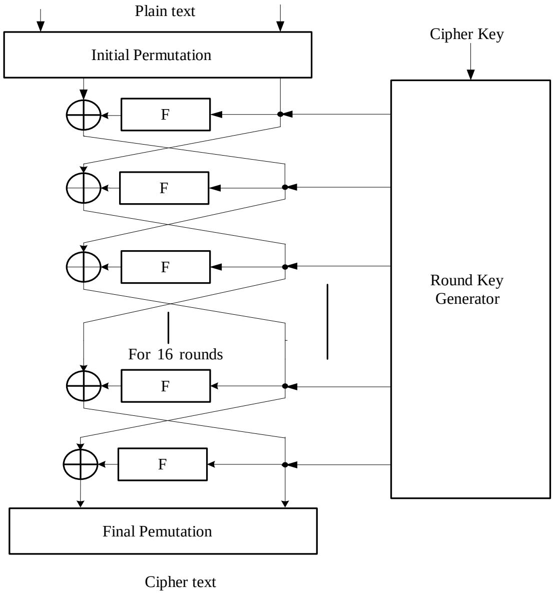


Fig 1.1: General block diagram of Data Encryption Standard (DES)

DOI 10.17148/IJARCCE.2018.713

B. Conventional Data Encryption Model

The conventional encryption model (as shown in fig 1.2) has five components. They are

1) *Plain text*: The plain text in cryptography (or encryption model) refers to the input text which is created (or stored) for the purpose of sending it a receiver. This block does not contain any prior encryption (in case of multiple encryptions the encrypted data in this block will be treated as plain text itself). The plain text acts as an input to the encryption algorithm. This is also sometimes referred to as clear text.

2) *Encryption algorithm*: The encryption process is a method used to encode the data in a way that only the intended or authorized person can read the intended data. The algorithm used for such purpose is called encryption algorithm. The system does not prevent interception of data but does not provide the actual content. The output produced by the encryption block is called as the cipher text.

3) *Cipher text*: This block contains the encrypted plain text which was transformed by the encryption block. This text which is called as the cipher text avoids an unauthorized person to access the original plain text.

4) *Key*: The key is the information which enables the intended receiver to decrypt the cipher text in order to access the original pain data. In general a key specifies the transformation between cipher data and original pain data.

5) *Decryption algorithm*: This is usually the inverse of the encryption algorithm, This is applied to retrieve back the original data from the ciphered data by using the key.

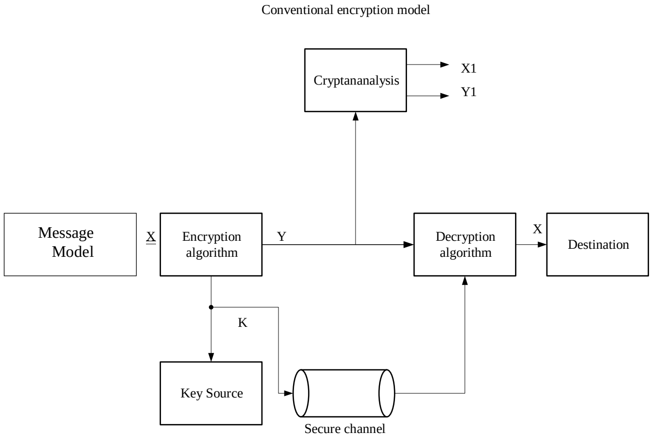


Fig 1.2: Conventional Encryption model Where, X→ data to be encrypted Y→ Cipher data K→ Algorithm key

C. Parameters Relating To Image Encryption

1) *Tunability*: The dynamic definition of the encryption parameters and the encrypted part according to various requirements and applications. Static definition of encrypted part and encrypted parameters helps in scalability for schemes usage.

2) *Cryptographic security*: This defines to know the security of encryption scheme against the plaintext attacks and brute force; and the security is measured as high, medium or low.

3) *Speed*: This defines the faster time for encryption and decryption processing of algorithms.

4) *Compression*: This helps in maintaining the bandwidth of the image while transmission and also helps during the decryption.

5) *Visual degradation* : This helps in the measurement of the image data perceptual distortion according to with plain image

D. Objectives

The primary objective of the proposed system is to perform multimodal based cryptographic key by addressing the following objectives.

1. To perform a study on biometric based cryptographic system
2. To perform fingerprint and palm print recognition
3. To perform performance validation of the proposed biometric based cryptographic system

DOI 10.17148/IJARCCE.2018.713

II. PROPOSED SYSTEM AND DESIGN DOCUMENT

A. General System Architecture

The purpose of the proposed model is to provide improved security with respect to uniqueness by considering the multimodal biometric system. Initially a database is created which comprises of the fingerprint and palmprint samples. Intensity transformation is performed with respect to gray scale values. The image segmentation is performed for the purpose of extracting the ROI in the palmprint and fingerprint. Consecutively the features are detected using the Gabor filter and minutiae; the features are then applied to a DWT based image fusion method followed by 256 key data encryption and decryption.

B. Data Flow Diagram

The data flow diagram is presented to illustrate the behavior of the data with respect to its transition from one block to another. The intention of this section is to provide the reader as to how the data transforms while being processed from one block to another. Two levels of dataflow is given in this section as shown below, the first level is the level 0 which explains the purpose of the proposed system. The second level is the level 1 which explains the functionalities associated with the system in order to obtain the proposed purpose.

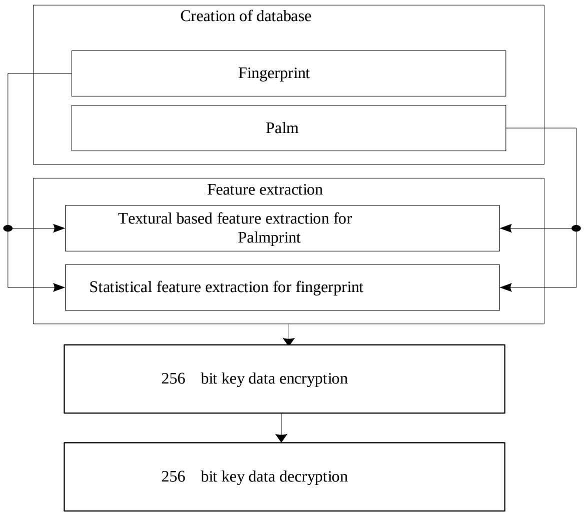

Creation of database
Fingerprint
Palm
Feature extraction
Textural based feature extraction for Palmprint
Statistical feature extraction for fingerprint
256 bit key data encryption
256 bit key data decryption

Fig 2.1: Proposed system architecture

1) *Level 0*: The purpose of the system is provide Identification and authentication for the system using a multimodal biometric system. By considering this method the overall uniqueness of the modal will increase. The level 0 dataflow diagram for the proposed system is as shown in fig 3.2.

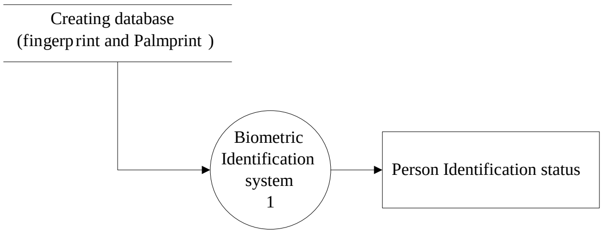

Creating database
(fingerprint and Palmprint)
Biometric Identification system
1
Person Identification status

Fig 2.2: Level 0 data flow diagram concerning the biometric identification system

2) *Level 1*: The basic functionality of the proposed system is to provide identification of an individual based on the fingerprint and palmprint of the person. The image is first performed segmentation following by ROI extraction. Consecutively feature extraction is performed using Gabor filter and minutiae for palmprint and fingerprint modalities respectively. The procedure is followed by image data fusion using DWT based method consider the ‘haar’ and ‘db8’ based basis function. The fused image is then encrypted using a 256 bit data encryption method. The level 1 data flow diagram considering the functionalities of the proposed system is shown in fig 3.3.

DOI 10.17148/IJARCCE.2018.713

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

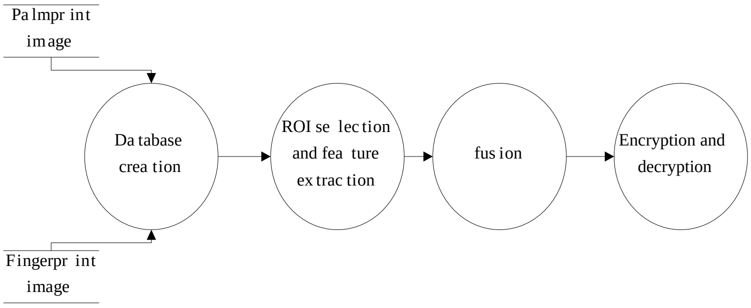

Palmprint image
Database creation
ROI selection and feature extraction
fusion
Encryption and decryption
Fingerprint image

Fig 2.3: Level 1 data flow diagram concerning functionalities of the proposed biometric system

C. Image Fusion Method Using Discrete Wavelet Transformation

Discrete Wavelet Decomposition

In the decomposition stage, a preferable technique used in decomposition stage is the Discrete Wavelet Transformation (DWT), the selection criteria for DWT was based on its computational efficiency, practicality and simplicity. The data flow diagram for wavelet decomposition is given in fig.3.4.

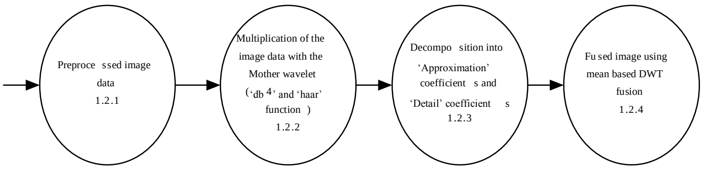

Preprocessed image data
1.2.1
Multiplication of the image data with the Mother wavelet (‘db 4’ and ‘haar’ function)
1.2.2
Decomposition into ‘Approximation’ coefficients and ‘Detail’ coefficients
1.2.3
Fused image using mean based DWT fusion
1.2.4

Fig 2.4: Data-flow diagram level-1 corresponding to the working of the wavelet decomposition method

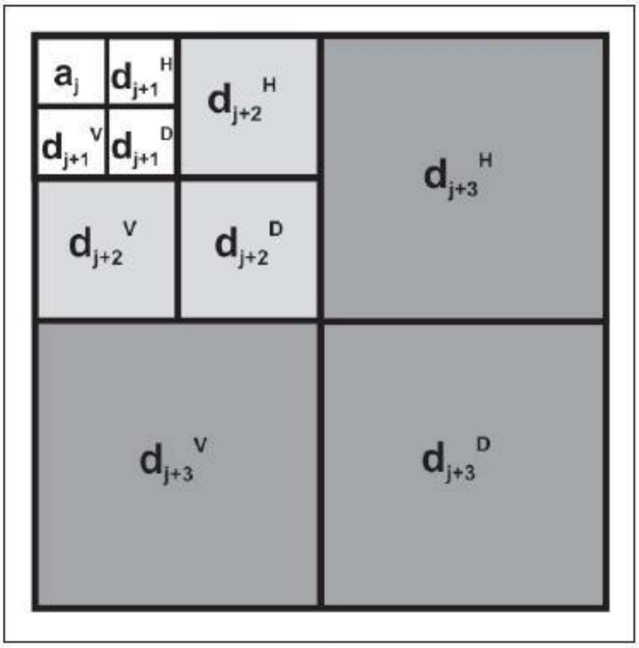


Figure 2.5: Two dimensional wavelet transformation

The pre-processed image data is further multiplied with the basis function considering the ‘haar’ and the ‘db4’. This results in two types coefficients mainly derived from low pass filter and the high pass filter known as Approximation Coefficients (AC) and the Detail Coefficients (DC) respectively. The decomposition is performed up to 3 level, however, this parameter could be adjusted considering the nature of image. The image fusion method considered in this context is the mean based image fusion. In this method, the mean of AC components of two images is performed, along with computing the mean of DC components of two images, upon reconstruction of the image (considering the updated AC and DC components) using the inverse DWT, the fused image is obtained.

DOI 10.17148/IJARCCE.2018.713

D. Process Flow For DWT Based Image Fusion

Decomposition of pre-processed for image fusion using DWT

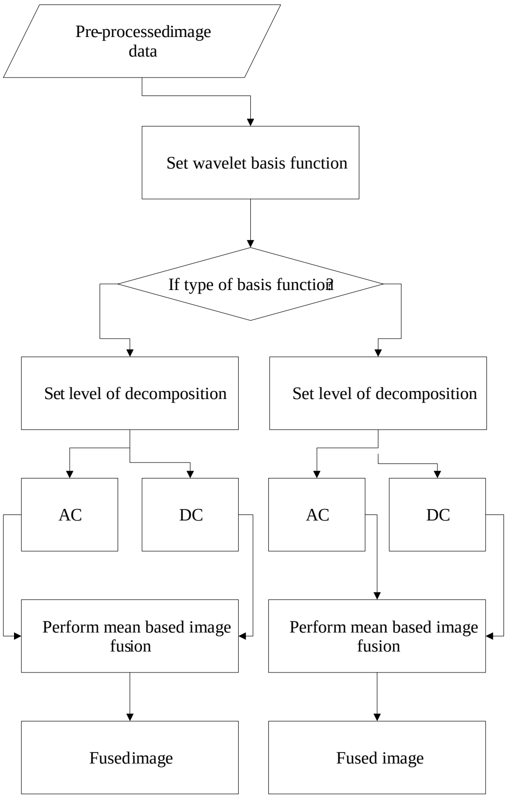

Pre-processedimage data
Set wavelet basis function
If type of basis function
Set level of decomposition
Set level of decomposition
AC
DC
AC
DC
Perform mean based image fusion
Perform mean based image fusion
Fusedimage
Fused image

Fig 2.6: Wavelet based decomposition for image fusion

Initially an input image (plain image) is resized to have an equal dimension of square matrix. A bit level encryption is performed where the key is generated having the same number of rows as the number of total bytes and the 1 column. Each bit in the plain image is XORed with the value of the corresponding position of the key. The resulting encrypted image is then sent to the chaotic based mapping encryption considering the scrambling method used to scramble a number of iteration for the bit is specified by the user. The key with respect to bit size is generated by first entering a value which in turn produces a random number, the value of this random number is considered as the number of iterations for the bit encryption method to be performed. The resulting image is the ciphered image which is expected to have a reduced correlation coefficient with respect to image pixels. The decryption of the image is performed by first considering the ciphered image obtained by the bit level decryption method. The user will be prompted for a key, this is the same key which was set during the encryption process. Upon entering the respective key the iteration value is retrieved which will perform the same number of iteration as was performed during the encryption process. The decrypted image from. Upon receiving the key the pixel position of the decrypted image is XORed with the corresponding pixel position of the key. The resulting image is the final decrypted image. The final decrypted image is sent to quality assessment which in turn assesses the quality of the image with respect to its psnr value. The level 2data flow diagram for the proposed system is shown in fig 3.7.

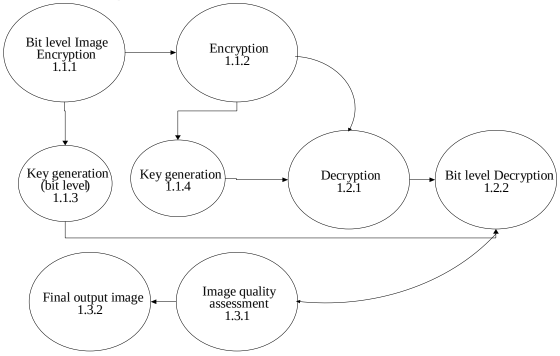

Bit level Image Encryption 1.1.1
Encryption 1.1.2
Key generation (bit level) 1.1.3
Key generation 1.1.4
Decryption 1.2.1
Bit level Decryption 1.2.2
Final output image 1.3.2
Image quality assessment 1.3.1

Fig 2.7: Level 2 data flow diagram mentioning the methods involved proposed system

DOI 10.17148/IJARCCE.2018.713

1) *Bit level encryption/ decryption process***:**

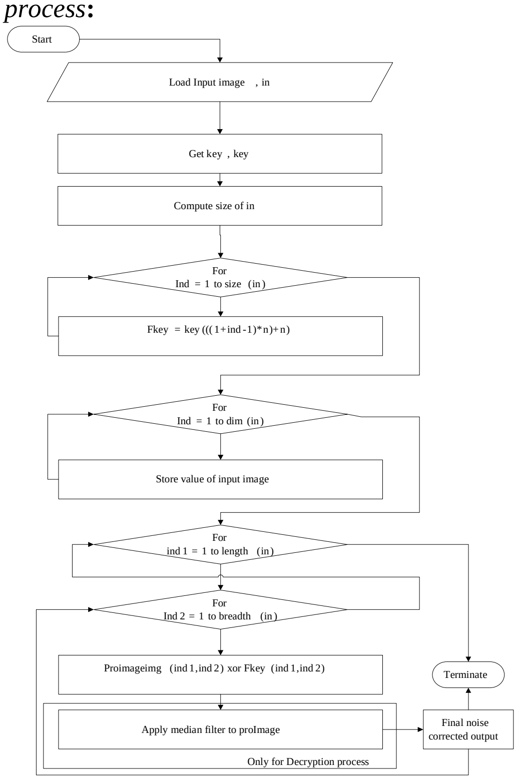

Start
Load Input image , in
Get key , key
Compute size of in
For
Ind = 1 to size (in)
Fkey = key (((1+ind -1)*n)+n)
For
Ind = 1 to dim (in)
Store value of input image
For
ind 1 = 1 to length (in)
For
Ind 2 = 1 to breadth (in)
Proimageimg (ind 1,ind 2) xor Fkey (ind 1,ind 2)
Apply median filter to proImage
Only for Decryption process
Terminate
Final noise
corrected output

Fig 2.8: Process flow diagram for the Bit level encryption/ decryption process

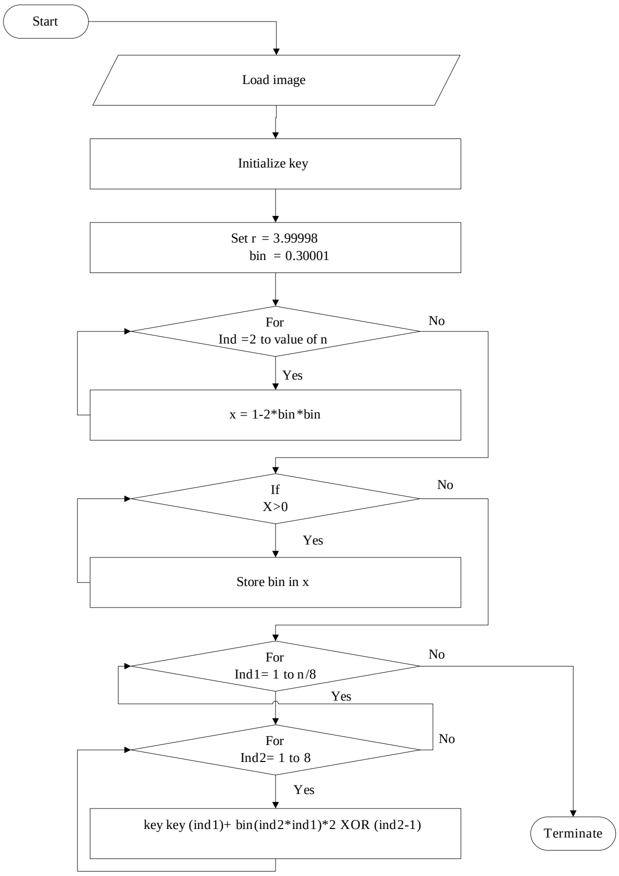


Fig 2.9: Process flow diagram for the key generation for the bit level encryption/ decryption process

DOI 10.17148/IJARCCE.2018.713

2) Key generation for the bit level encryption/ decryption process

E. Introduction

In a view to extend the applications of image processing towards a broader perspective, one application is concerned with the intention of providing an enhanced security with respect to uniqueness. Many algorithms has been developed with respect to this area, one such particular instance is the multimodal biometric system.

F. Intended Audience

This document is intended for the technically oriented people such as Project Guide who may insist and evaluate the entirety of the project with respect to design considerations and result evaluations of this project.

Evaluation committee may use this document to evaluate the requirement specification and verify the correctness, completeness and absolute requirements. Peers may review this document concerning the design considerations, parametric evaluations and scope of the project and could further enhance the project with respect to above parameters.

G. Overall Description

The software requirement specification gives the information of the system with respect to its behaviour. Accordingly this document consists of classes that illustrate all the requirements for the interactions between user and software. The topics covered in this document include a view of the project in a product perspective which gives a general description of the overall system and its significance, User characteristics which indicates the user necessary technical requirement and the knowledge required to understand and operate the system, describing the functional requirements of the system with respect to quality standards, design drawbacks and performance evaluation and non-functional requirements concerning the usability, security, maintainability, availability, portability, integrity and extensibility of the system.

H. Product perspective

In a view to provide a more enhanced security with respect to uniqueness, A multimodal biometric system considering the fingerprint and palm print modals are used. The process is first described by creating a user database, performing image segmentation (extracting Region Of Interest - ROI) and consequently feature extraction, fusion and finally process of data encryption.

I. User Characteristics

The pre-requisites for the user for the understanding and operation of the system are as follows.

The users should have an understanding of the basics and working of Matlab along with the knowledge of using the inbuilt methods and functions in it.

The user should possess knowledge and understanding of basic image processing functions and applications.

J. Functional And Non-Functional Requirement The functional and Non-functional description provided below describes the general operation of the system proposed in this project. A thorough understanding of these two topics will enable the user to understand and operate the system more effectively.

1) *Functional requirement*: The database is created in the system considering the palm and fingerprint of the individual, image segmentation is performed for both the images in order to extract the ROI, feature extraction is performed based on the Gabor filter and Minutiae, fusion is performed using DWT and finally encryption is performed using 256 bit key.

2) *Non-Functional requirement*:

Usability: The system will be able to identify the physiological structure of the fingerprint and palmprint provide recognition respectively. The Uniqueness is considerably improved considering the parameter of multimodality.

Availability: The scheme will be available at all time for the user to operate and verify the result of the system.

Portability: The system is designed with Matlab as a platform which has compatibility towards multiple operating systems having Matlab preinstalled in them.

Integrity: The project is designed in Matlab IDE consisting of many toolboxes, building and debugging the main class will integrate all classes accordingly for proper compilation of the project. Extensibility: The Project has also been provided provisions which would allow for future modifications, thus enhancing the scope of the project.

K. Interface Description

This section tells the user his range and scope of controlling the parameters and performing operations with respect to the system designed. In simpler words it provides a bridge between the user and the system.

L. User Interface

A graphic User Interface is created in Matlab for the user for the purpose of giving inputs, adjusting parameters and analysing the obtained results.

M. Software Interface

The system designed herein has no constraints on operating systems as long the corresponding OS supports Matlab. The OS could be Windows, MAC or Linux to name a few. Hardware Interface. The hardware used in this project is a 64 bit Windows operating system supported by an Intel 1st generation i3 processor along with an NVIDIA graphic card of 1GB capacity with 4GB of Internal memory.

III. RESULTS AND DISCUSSIONS

The evaluation methodologies followed in this experiment are as follows,

1. Peak signal to noise ratio (PSNR): frequently curtailed PSNR, is a defining term for the proportion between the greatest conceivable energy of a signal and the energy of undermining commotion that influences the loyalty of its portrayal. Since many signs have a wide unique range, PSNR is typically communicated as far as the logarithmic decibel scale.
2.
3. Signal to Noise Ratio (SNR) : Signal-to-noise ratio is defined as the ratio of the power of a signal (meaningful information) and the power of background noise (unwanted signal)

$$SNR = \frac{Psignal}{Pnoise}$$

Where, P is average power. Both signal and noise power must be measured at the same and within the same system bandwidth.

A. Adjacent Pixel Correlation Analysis

Connection is a measure of the connection between two factors or pixels in a picture. On the off chance that the two pixels are the two neighboring pixels in a picture, at that point there is a nearby relationship between them else it is said they are less associated. This is called nearby pixel relationship in a picture. The connection coefficient CC, is registered the estimations of two contiguous pixels in the first and encoded picture and N is the aggregate number of nearby pixels chose from the picture additionally alluding to mean. On account of an encoded picture, the contiguous pixel connection will be less if the encryption procedure is equipped for concealing the points of interest of the first picture. The main GUI block representing the entire module considering feature extraction, fusion and encryption methods is given in fig 3.1 as shown

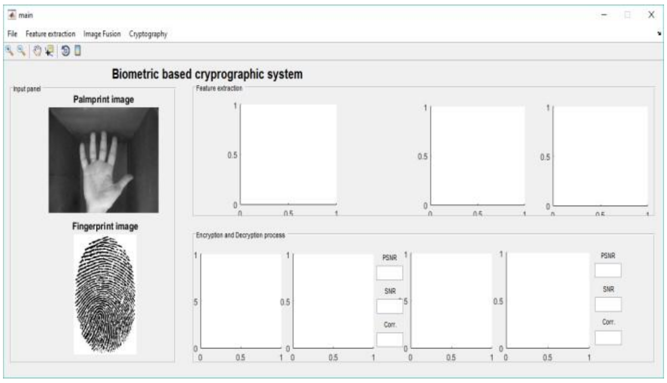


Fig 3.1: Main GUI

The palm print image is loaded, and is subsequently, prompted to select a region of interest, for further extraction of feature based on the textural context of the palm print module. The filter used is the 2D dimensional Gabor filter that which produces the phase and magnitude of the acquired image (as shown in fig 5.2).

DOI 10.17148/IJARCCE.2018.713

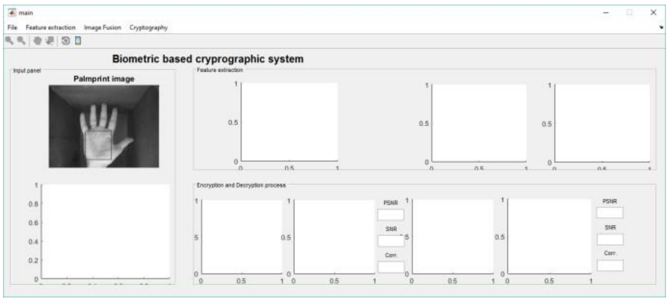
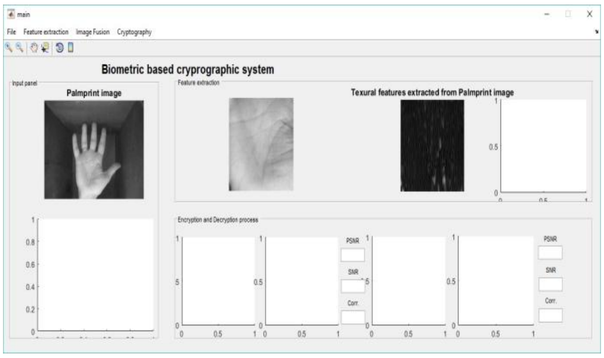

main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Feature extraction
Encryption and Decryption process
PSNR
SNR
Corr.

Fig 3.2: Extracting region of interest for palm print image


main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Feature extraction
Texural features extracted from Palmprint image
Encryption and Decryption process
PSNR
SNR
Corr.

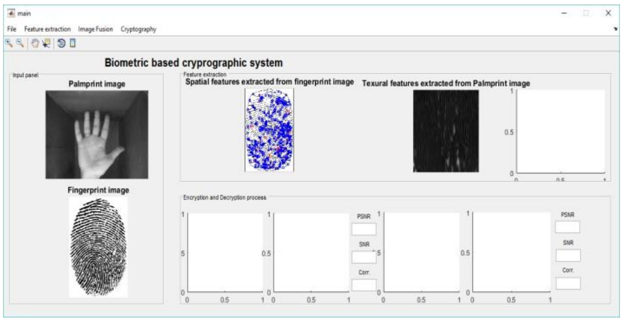

main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Fingerprint image
Feature extraction
Spatial features extracted from fingerprint image
Texural features extracted from Palmprint image
Encryption and Decryption process
PSNR
SNR
Corr.

Fig 3.6: Extracting minutiae based features for finger print image

Fig 3.3: Palm print region selected by user for textural feature extraction The two obtained images are then fused using the DWT based   method considering the db8 as the basis function as shown in fig 5.7 respectively.

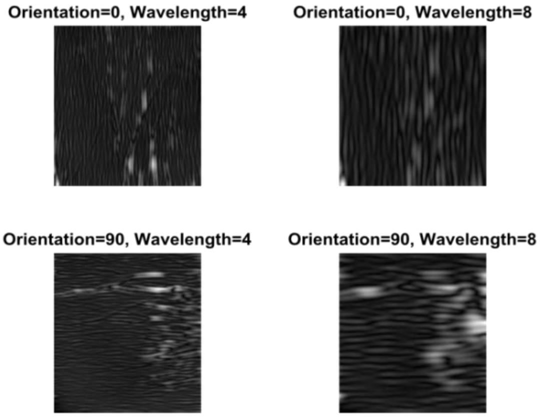

Orientation=0, Wavelength=4
Orientation=0, Wavelength=8
Orientation=90, Wavelength=4
Orientation=90, Wavelength=8

Fig 3.4: Gabor filter coefficients for palm print image

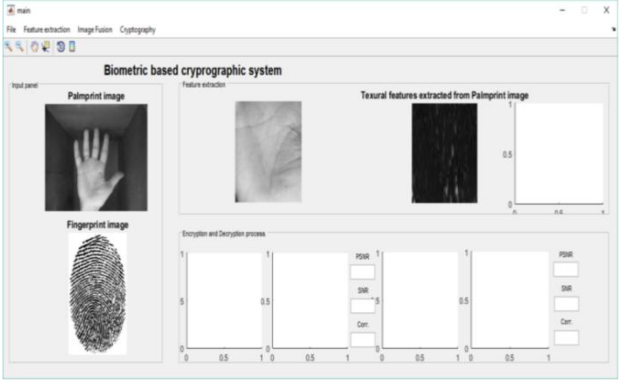

main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Fingerprint image
Feature extraction
Texural features extracted from Palmprint image
Encryption and Decryption process
PSNR
SNR
Corr.

Fig 3.5: Loading of finger print image

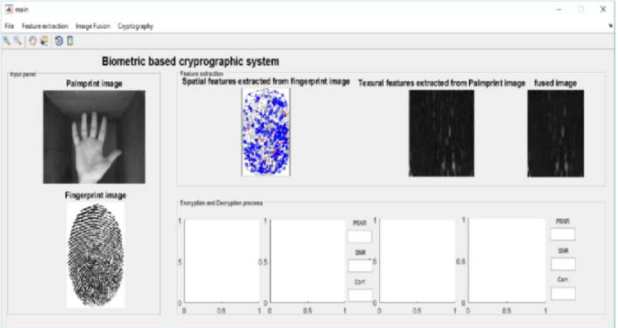

main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Fingerprint image
Feature extraction
Spatial features extracted from fingerprint image
Texural features extracted from Palmprint image
fused image
Encryption and Decryption process
PSNR
SNR
Corr.

Fig 3.7: Image fusion of palm print and fingerprint modality using DWT method

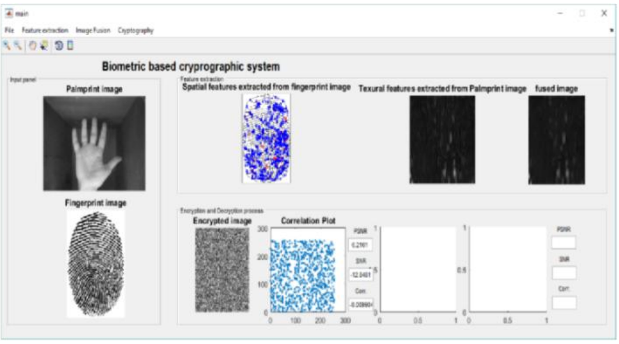
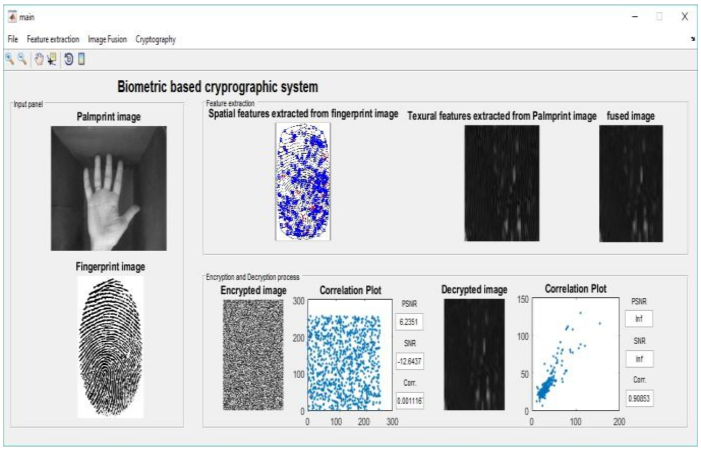

main
File Feature extraction Image Fusion Cryptography
Biometric based cryprographic system
Input panel
Palmprint image
Fingerprint image
Feature extraction
Spatial features extracted from fingerprint image
Texural features extracted from Palmprint image
fused image
Encryption and Decryption process
Encrypted image
Correlation Plot
PSNR
SNR
Corr.

Fig 3.8: Encryption for the fused image

Similarly, the finger print image is loaded and the statistical features concerning the minutiae based feature extraction is procured which is shown in fig 3.6 as follows.

DOI 10.17148/IJARCCE.2018.713



PSNR 6.2351
SNR -12.6437
Corr. 0.001116

PSNR Inf
SNR Inf
Corr. 0.90853

Fig 3.9: Decryption for the fused image

Furthermore, the encryption and decryption methods are performed considering the 256 bit key for information retrieval, The correlation plot along with image quality assessment such as PSNR, SNR and correlation coefficient before and after encryption and decryption process is performed (as shown in fig 3.8 and 3.9 respectively).

Table I PSNR, SNR and Correlation Coefficient Before and After Encryption and Decryption Process

S.no	Image	image type	PSNR	SNR	corr. coef
1	image1	uint8	7.9583	-0.05	-0.02 0.93
2	image2	uint8	7.84	-0.84	-0.03 0.92
3	image3	uint8	7.78	-2.24	0.019 0.91
4	image4	uint8	7.79	-1.89	-0.05 0.911
5	image5	uint8	7.74	-2.21	-0.01 0.91

IV. APPLICATIONS, ADVANTAGES AND DISADVANTAGES

A. Applications

Combination of cryptography and biometrics highly secures the data information and hence has been widely used by businessmen owning various internet services such as banking, internet shopping, tax filling, web mail, subscriptions of newspaper and magazines electronically, gaming. The services are protected from fraudulent activities by those individuals who do not pay and those who carry out other types of illegal activities.

They are currently used in identity cards by many countries and thus helps in mitigating the threat of terrorism.

The data information are made to be stored at large locations that is to be present and available everywhere and hence the applications has extended from the crime area (forensic area) to the civil area in order to prevent criminal activities.

Password-based authentication is getting replaced by biometric-based authentication in those areas where passwords were used to secure individual’s information previously. Forgery and counterfeiting of secured items cannot be done in this and hence used in such areas which demands for its security.

B. Advantages

Combining cryptography and biometrics has the ability to link an individual with a digital signature the person creates with high degree of assurance.

Comparatively biometric authentication is more reliable than password-based authentication, the reason being that the biometric characteristics cannot be lost or forgotten; it is a daunting task to share, copy, distribute and require the person being authenticated to be present at the time of authentication.

It is not very easy to forge biometrics.

It is unlikely for the user to repudiate having accessed the digital content with the usage of biometrics. An individual’s biometrics is no easier to be cracked than another’s.

DOI 10.17148/IJARCCE.2018.713

C. Disadvantages

One of the issues with the approach is its dependence on hardware tamper-resistance; In case the token is broken, both the template and key are lost. Therefore better way of combining cryptography, biometrics and tamper-resistance are looked for. Main obstacle is that biometric data are noisy and only an approximate match can be expected to a stored template and cryptography requires exact key which otherwise fails the protocol.

V. CONCLUSION AND FUTURE ENHANCEMENT

A. Conclusion

From the proposed experiment, we have performed textural based feature extraction for palm print image using Gabor filter and minutiae based feature extraction for finger print extraction. Both templates are fused using DWT based fusion method. The fused image is further encrypted using 256 bit based encryption method, upon the activation of key, the ciphered data is decrypted. The overall correlation factor achieved post decryption was 0.9085 with improved SNR and PSNR values.

B. Future Enhancement

The future enhancement lies in reduction of multiple sensors and addition of optimization algorithm for the selection and matching of the features. This biometric based cryptographic security can be integrated to e-governance and e-health management.

REFERENCES

[1] K. Jain, A. A. Ross, and K. Nandakumar, "Introduction to Biometrics." *New York, NY, USA: Springer-Verlag,2011*

[2] H. Liu and L. Yu, "Toward integrating feature selection algorithms for classification and clustering," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 4, pp. 491–502, Apr. 2005.

[3] M. A. Hall, "Correlation-based feature selection for discrete and numeric class machine learning," in *Proc. 17th Int. Conf. Mach. Learn.*, 2000, pp. 359–366.

[4] L. Yu and H. Liu, "Efficient feature selection via analysis of relevance and redundancy," *J. Mach. Learn. Res.*, vol. 5, pp. 1205–1224, Oct. 2004. [5] L. Wang and G. Leedham, "A thermal handvein pattern verification system," in Pattern Recognition and Image Analysis, S. Singh, M. Singh, C. Apte, and P. Perner, Eds. New York: Springer, 2005, vol. 3687, pp. 58–65.

[6] C.-L. Lin and K.-C. Fan, "Biometric verification using thermal images of palmdorsa vein patterns," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 2, pp. 199– 213, Feb. 2004.

[7] J. M. Cross and C. L. Smith, "Thermo graphic imaging of the subcutaneous vascular network of the back of the hand for biometric identification," in Proc. IEEE 29th Annu. Int. Carnahan Conf. Security Technology, Sander-Stead, Surrey, U.K., Oct. 1995, pp. 20–35

[8] M. Khan and N. Khan, "A New Method to Extract Dorsal Hand Vein Pattern using Quadratic Inference Function", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 6, No. 3, 2009

[9] Miloš Oravec, "Feature Extraction and Classification by Machine Learning Methods for Biometric Recognition of Face and Iris", *Institute of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak*

[10] Sahu, Deepak Kumar, and M. P. Parsai. "Different image fusion techniques–a critical review." *International Journal of Modern Engineering Research (IJMER)* 2.5 (2012): 4298-4301.

[11] Zhang, Yun. "Understanding image fusion." *Photogrammetric engineering and remote sensing* 70.6 (2004): 657-661.

[12] Gross, Harry N., and John R. Schott. "Application of spectral mixture analysis and image fusion techniques for image sharpening." *Remote Sensing of Environment* 63.2 (1998): 85-94.

[13] Alparone, Luciano, et al. "A global quality measurement of pansharpened multispectral imagery." *IEEE Geoscience and Remote Sensing Letters* 1.4 (2004): 313-317.

[14] González-Audícana, María, et al. "Fusion of multispectral and panchromatic images using improved IHS and PCA mergers based on wavelet decomposition." *IEEE Transactions on Geoscience and Remote sensing* 42.6 (2004): 1291-1299.

[15] Choi, Myungjin. "A new intensity-hue-saturation fusion approach to image fusion with a tradeoff parameter." *IEEE Transactions on Geoscience and Remote sensing* 44.6 (2006): 1672-1682.

[16] Z. Dinghui, G. Qiujie, P. Yonghua, and Z. Xinghua, "Discrete chaotic encryption and decryption of digital images," *in Proc. Int. Conf. Comput. Sci. Soft. Eng., Wuhan, China*, pp. 849–852, 2008.

[17] J. Zhou, X. Liu, O.C. Au, and Y.Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation," *IEEE Trans. Inf. Foren. Sec.*, vol. 9, no. 1, pp. 39– 50, 2014.

[18] Sk. Md. Mizanur Rahman, M.A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "Chaos-cryptography based privacy preservation technique for video surveillance," *Multim. Sys.*, vol. 18, no. 2, pp. 145– 155, 2012.

[19] T. Uehara and R. Safavi-Naini, "Chosen DCT coefficients attack on MPEG encryption schemes," in Proc. *IEEE Pacific Rim Conf. Multim.* (IEEE-PCM'2000), pp. 316–319, 2000.

[20] L. Zhao, A. Adhikari, D. Xiao, and K. Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption," *Comm. Nonlinear Sci. Numer. Simulat.*, vol. 17, no. 8, pp. 3303–3327, 2012.

[21] X.-Y. Zhao, G. Chen, D. Zhang, X.-H. Wang, and G.-C. Dong, "Decryption of pure-position permutation algorithms," *J. Zhejiang Univ. Sci.*, vol. 5, no. 7, pp. 803–809, 2004.

[22] Y. Matias and A. Shamir, "A video scrambling technique based on space filling curves," in Proc. *Advances in Cryptology–Crypto'87, Lecture Notes in Computer Science*, vol. 293, C. Pomerance, Ed., Springer, pp. 398–417, 1987.

[23] M. Bertilsson, E.F. Brickell, and I. Ingemarson, "Cryptanalysis of video encryption based on space-filling curves," in Proc. *Advances in Cryptology–EuroCrypt'88, Lecture Notes in Computer Science,* vol. 434, Springer, Berlin, pp. 403–411, 1989.

[24] M. Kuhn, "Analysis for the Nagravision video scrambling method," *1998, online document,* available at: http://www.cl.cam.ac.uk/ mgk25/ nagra.pdf.

[25] J. McCormac, European Scrambling Systems 5: Circuits, Tactics And Techniques – The Black Book, Waterford University Press, 1996.

[26] W. Li, Y. Yan, and N. Yu, "Breaking row-column shuffle based image cipher," in Proc. *20th ACM international conference on Multimedia (MM'12), New York, NY, USA*, pp. 1097–1100, 2012.

DOI 10.17148/IJARCCE.2018.713