ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Security on Fingerprint Data Transfer System

Hinal Modi[1], Darshana Mistry[2]
[1]IT System & Network Security, Gujarat Technological University, India
[2]Technical Associate, Elnfochips Training & Research Academy, India

Abstract: Nowadays, the data can undergo grave modifications (access to the credit cards, the transactions in e-commerce, espionage of the secret information in military domain, theft biometrics information) especially through transmissions on the insecure network or internet. Where, it is necessary to look a robust method to secure the data. In this work we are focusing on matching data pattern along with all security assurance, so that we can provide discrete wavelet transform watermarking and en-decryption using confusion and diffusion method. The encryption method is based on XORing the message bytes and, it is the key used for encryption and decryption that makes the process of cryptography secure because key was automatically taken by system. Its performance with biometric information (fingerprint) using MATLAB 7.10(R20109).

Keywords: Fingerprint, Watermarking, Discrete Wavelet Transform, Confusion and Diffusion

I. INTRODUCTION

Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. Biometric systems use a person's physical characteristics (like fingerprints, irises or veins), or behavioral characteristics (like voice, handwriting or typing rhythm) to determine their identity or to confirm that they are who they claim to be. The most widely used biometric technology is the fingerprint system. Their stability and uniqueness make the fingerprint identification system extremely reliable and useful for security applications [2].

II. FINGERPRINT

A fingerprint is comprised of a pattern of lines, known as ridges. The spaces between individual ridges are referred to as valleys. Among the variety of minutia types, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive [1].

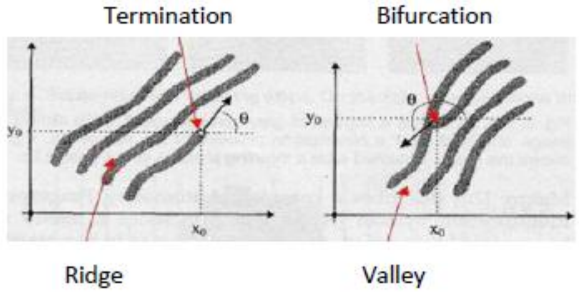

Figure 1: Minutia

III. FINGERPRINT APPLICATION

Fingerprint based biometrics has primarily been used to secure entry devices for building door locks and computer network access. A small number of banks use fingerprint readers for authorization at ATMs. Grocery stores are experimenting with a fingerprint scan checkout that automatically recognizes and bills a registered user's credit card or debit account. More recent applications of finger recognition include use of fingerprints for voter registration.

The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.

- Banking system-ATM security, card transaction
- Physical access control(airport)
- Information system security
- National ID system
- Identification of criminal

IV. FINGERPRINT METHODS

There are three main methods for fingerprint matching which are correlation based matching, minutiae based matching, pattern based matching.

Comparison of Method:

The correlation-based fingerprint verification is compared to the traditional minutiae-based methods. The advantages of the correlation based over minutiae based method are:

- The method uses the much richer gray-level information of the fingerprint image instead of only positions of minutiae.
- The method is also capable of dealing with fingerprints of bad image quality from which no minutiae can be extracted reliably.
- False and missed minutiae do not decrease the matching performance.
- Unlike the minutiae templates, the template locations are already paired, which results in much simpler matching methods. When registering minutiae sets, it is not known in advance which minutiae from both sets should correspond.
- The first decision stage only classifies relative template positions. This method tolerates non-uniform local shape distortions in the fingerprint, unlike the minutiae templates for which the optimal global transform is searched.

The disadvantages of the correlation-based over minutiae extraction technique fingerprint verification method are:

- Template matching is a method that demands a rather high computational power, which makes the method less applicable for real time applications.
- The method is at the moment not capable of dealing with rotations of more than about 10 degrees. This is caused by the fact that, for larger rotations, the templates doesn't match well anymore, causing incorrect positions to be found. A solution to this problem is rotating the templates and then performing the matching again. However, this is a solution that requires a lot of additional computational power.
- Problems might arise if the minutiae-based or coherence-based template selection methods are used while 2 minutiae surroundings resemble a lot. In this case, there is a probability that template matching will find the incorrect template position, which degrades the matching performance. Use of the correlation characteristic template selection will solve this problem [10].

The advantage of Pattern Matching techniques over Minutiae Extraction is that minutiae points may be affected by wear and tear and the disadvantages are that these are sensitive to proper placement of finger and need large storage for templates.

V. WATERMARKING

Watermarking is the method to hide the secret information into the digital media using some strong and appropriate algorithm. Algorithm plays a vital role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain.

a) **Spatial domain:** This domain focuses on modifying the pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels, such as LSB.

b) **Frequency domain:** This technique is also called transform domain. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT [3].

Algorithm	Advantages	Disadvantages
LSB	1.Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions.	1. Complex implementation 2. Cost of computing may be higher.

Discrete wavelet transforms (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL).

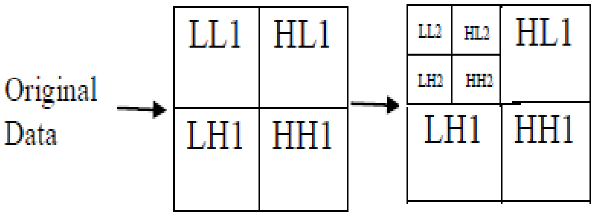

Figure 2: Frequency distribution after DWT

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [4].

VI. CRYPTOGRAPHY

Most of the existing encryption algorithms are best suited for textual data and cannot directly be applied on images since image data have special features such as bulk capacity, high redundancy and high correlation among pixels that imposes special requirements on the encryption technique used. Therefore, image security has its own special requirements that lead to different thoughts to protect digital data. There are main two domain of cryptography, symmetric key and asymmetric key cryptography. There are so many algorithms such as AES, DES, RSA etc. but they take more computational time to encrypt and decrypt the image. It is symmetric algorithm. Claude Shannon introduced the concept of confusion and diffusion, which are significant from the perspective of computer-based cryptographic techniques. It is symmetric algorithm.

Confusion is the process of hiding the plain image. In this algorithm Confusion is performed by bit XORing first pixel of red channel of the image with key K1, first pixel of green channel with K2, first pixel of blue channel of the image with key K3 and the other pixels will be XORed respectively.

R(1,1)= R(1,1)XOR k1
G(1,1)= G(1,1)XOR k2
B(1,1)= B(1,1)XOR k3
R(1,2)= R(1,2)XOR k4

The process will continue till all the pixels of R,G,B channel are XORed. After confusion, diffusion process is used. In diffusion process the output bits should depend on the input bits in a very complex way. To achieve this, in this algorithm diffusion process is carried out in two steps i.e. horizontal diffusion and vertical diffusion.

Horizontal diffusion

This is one of the techniques used in this algorithm. In horizontal diffusion each pixel is bit XORed with the next pixel row wise. Starting from the second pixel of red channel, the first pixel of the red channel is XORed with the second pixel and in the same way all the three channels are horizontally diffused.

R(i,j+1)= bitxor (R(i,j+1,1),R(i,j,1));
G(i,j+1,2)= bitxor (G(i,j+1,2),G(i,j,2));
B(i,j+1,3)= bitxor (B(i,j+1,3),B(i,j,3));

Vertical diffusion

Vertical diffusion starts with the last pixel. In Vertical diffusion the second last pixel of the R channel is bit XORed with the last pixel of G channel and B channel respectively whole channel is XORed. The second last pixel of the G channel is bit XORed with the last pixel of R channel and B channel respectively whole channel is XORed and the second last pixel of the B channel is bit XORed with the last pixel of R channel and G channel respectively whole channel is XORed[5].

R(i-1,j)=bitxor (R(i-1,j),G(i,j),B(i,j));
G(i-1,j)=bitxor (G(i-1,j),R(i,j),B(i,j));
B(i-1,j)=bitxor (B(i-1,j),R(i,j),G(i,j));

VII. PROPOSED SYSTEM

In this report, the proposed system would overcome the problem of integrity and authentication. For integrity, here we have used wavelet transform watermarking method and for authentication, we have used timestamp. We were adding timestamp in encryption as key.

Basic steps are used to apply DWT in Matlab

1. Read an image.
2. Convert an input image into a gray scale image.
3. Perform a single-level wavelet decomposition (we get for information approximation, horizontal, vertical and diagonal details of an image)
4. Construct and display approximations and details from the coefficients.
5. To display the results of the level 1 decomposition.
6. Reconstruct the original image from the decomposition.

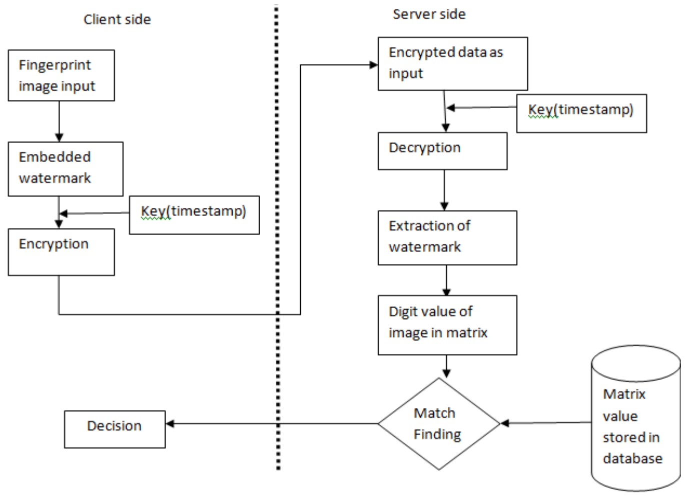

Figure 3: Proposed System

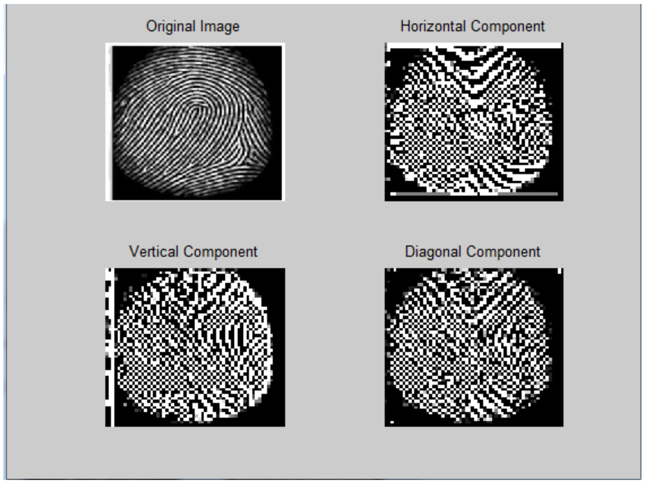

Figure 4: original image, DWT image based on approximate image detail (LL), horizontal details(HL), vertical details(LH) and diagonal details(HH) in one level.

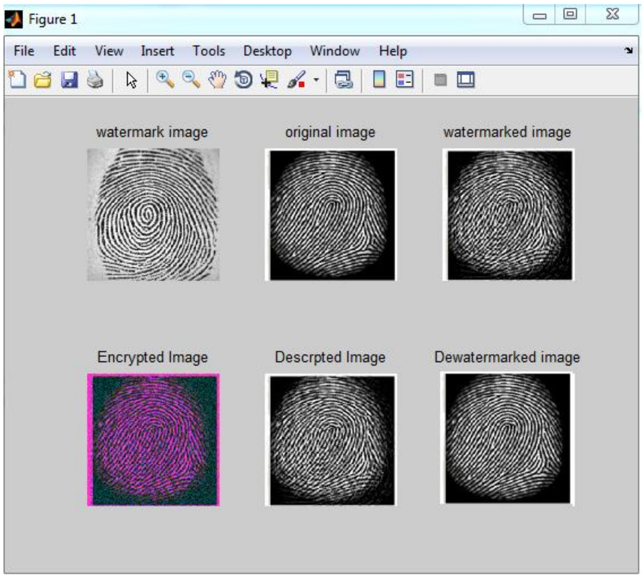

Figure 5: Output of proposed system

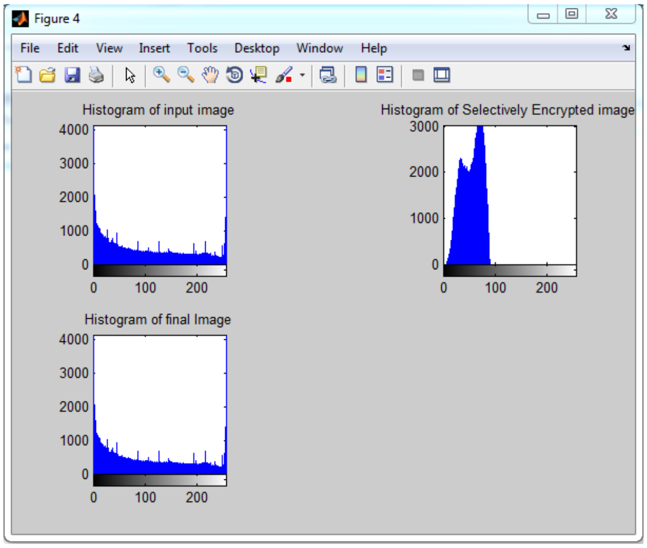

Figure 6: Histogram of Image

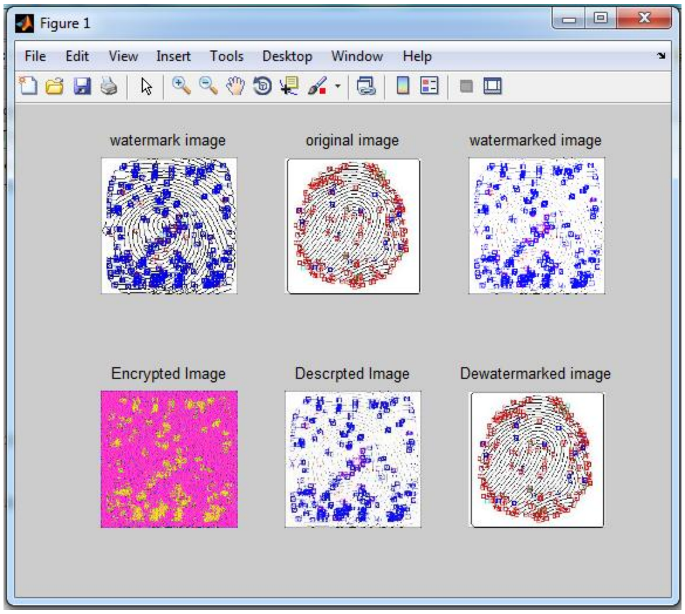

Figure 7: Output with PSNR value

Image Size	PSNR	MSE	Time
256*256	51.0737	0.5078	0.4394
223*226	51.0512	0.5105	0.4303

VIII CONCLUSION:

In this paper, we are providing a security, confidentiality and authentication over bio-metric information when it transmitted over unreliable channel. We have proposed a novel approach for grayscale-image encryption and decryption using confusion and diffusion associated with discrete wavelet transformation. Additionally, although, attacker try about the all possible correct keys, but not able to know about the correct key, because key was time based and its change according to system time, so attacker cannot decrypt the image correctly. This method provides decryption with no information loss. So this approach can be used for transmission of grayscale-image data efficiently and securely through unsecured channels without loss of any information and intensity.

ACKNOWLEDGEMENTS

I would like to thank my guide, Prof. Darshana Mistry (CSE), for her professional leadership and valuable advice throughout my research work

REFERENCES

[1] Wuzhili, "Fingerprint Recognization", April 2002.

[2] Graig T. Diefenderfer," Fingerprint Recognition" , Master's Thesis, June 2006.

[3] Prabhishek Singh and R S Chadha , "A Survey of Digital Watermarking Techniques, Applications and Attacks ", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013.

[4] Darshana Mistry, Asim Banerjee, "Discrete Wavelet Transform Using Matlab" International Journal Of Computer Engineering & Technology, Volume 4, Issue 2, March – April (2013), pp. 252-259

[5] Atual kahate In cryptography and network security, 2nd Edition, Tata McGraw Hill Publishing Company Limited, New Delhi, 2008

[6] Darshana Mistry, Asim Banerjee, "Discrete Wavelet Transform Using Matlab" International Journal Of Computer Engineering & Technology, Volume 4, Issue 2, March – April (2013), pp. 252-259.

[7] Narshingha P V ,"Security of Data Transfer Over Insecure Channel Through Stenography", International Journal of Combined Research & Development , Volume: 1; Issue: 2; June –2013

[8] Akshya Kumar Gupta And Mehul S Raval, "A Robust and Secure Watermarking Scheme Based on Singular Values Replacement",Indian Academy of Sciences, Vol. 37, Part 4, August 2012, pp. 425–44

[9] P.Vijayram Reddy , K.Venkatesh Sharma , P. Mallesham And P. Radhadevi ,"Secure Image Transmission through Unreliable Channels ", International Journal on Computer Science and Engineering Vol. 02, No. 06, 2010, 2053-2058.

[10] Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, Leo P.J. Veelenturf and Berend Jan van der Zwaag , "A Correlation-Based Fingerprint Verification System " ,ProRISC 2000 Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 2000.