Mili Singh* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.3, April – May 2016, 3042 – 3047.

Self Embedding Fingerprint Watermarking and Steganography using LSB,RSA, 3-DWT and MLPSVM Algorithm

MILI SINGH
Research Scholar, Pacific Academy of Higher Education and Research University, Udaipur, India

Dr. JITENDRA SHEETLANI
Dean of Computer Application,Associate Professor Sri Satya Sai University of Technology & Medical Science, Sehore, India

Abstract—**Digital watermarking methods are used to biometric document protect from attacks of either intentional and accident. These attacks are intended to either circumvent the afforded security throughsystem or to normal functioning deter of the system.In this research,verification of fingerprint methods with watermarking technology combination to provide copyright protection and authentication of digital images is proposed. In proposed algorithm for higher performancepresent self embedding fingerprint watermarking and steganography using least significant bit (LSB), RSA, three level discrete wavelet transform (DWT) and multilayer perceptron support vector machine (MLPSVM) classification. In this study, we take cover image and create self watermark images using bi-cubic interpolation (BCI) method for memory saving.The proposed approach gives perfect results from previous work. The experimental database contains 3 person fingerprint images with 8 different images. In this study, we calculate false matching ratio (FMR), false rejection ratio (FRR), accuracy, time and peak signal noise ratio (PSNR). The experimental outcomes for FMR and FRR is 0.5833and 0.7500. PSNR value is varying from 70-95%. Accuracylies between 0 and 3. Also, we applied attacks on watermarked image (like noise and rotate). Also, calculate time of each image and it lies between 65-76%.**

Keywords—**DWT;RSA;LSB; PSNR;ACCURACY; MLPSVM; FMR; FRR;**

I. INTRODUCTION

Biometrics based systems of authentication have essentialbenefit over classicaluser identification techniques.

A fingerprint is the one finger pattern feature [1]. It is believed with strong confirmations that every fingerprint is unique. Each person has his own identifications with permanent individuality. So fingerprints have been for forensic investigation and identification used for a long duration of time [2].

Fig. 1 A fingerprint image acquired by an Optical Sensor

A fingerprint is a pattern of ridges and furrows which have average width and are parallel aligned to each other[4].

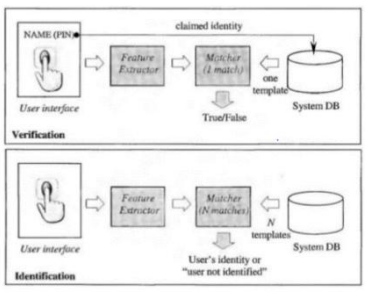


Fig 2. Fingerprint Identification vs. Fingerprint Verification

The recognition of fingerprint can be divided into two categories: one is verification of fingerprint and other is fingerprint identification[3]. Verification of fingerprint is to authentication verify of one person using his fingerprint[9]. The fingerprint verification scheme retrieves the template of fingerprint image and template image matches with the real-time captured fingerprint through the user. On the other side, each fingerprint recognition scenarios, either fingerprint verification or identification are based on a fingerprint template. The matching of fingerprint, for the 1- to-1 case of verification or 1-to-m identification case, is straightforward and simple.

However, there are various applications where this close relation between the person and its biometric signature is undesirable.[1]The first method is spread-spectrum watermark has low information capacity, next is a quantization watermark technique has low robustness, but have high information capacity, the last is amplitude modulation similar to spread spectrum technique but is mainly embedded in spatial domain. DWT, image Domain encoding which is called Least Significant Bit (LSB) techniques used for watermarking, but they have some backdrops as: Scope, tamper proofing, inseparability, transparency/visibility, and insecurity. [2]FHT has advantages over DWT at a short processing time, invisibility of watermark guaranteed, increase watermark energy leads to high robustness. RSA is an encryption calculation forcryptography ofpublic key based into the practical difficulty issue of factorization of substantial numbers as was depicted

by (Nasir & Kuppuswamy, 2013). RSA algorithm's introduction was in 1978 when it was initially presented by Rivest, Shamir and Adleman and was named after their names i.e. Rivest, Shamir and Adleman. The usage of RSA calculation includes an open key and a private key where the general population key can be known not and utilized for encoding messages. The feature image is created from input image as follows. First, the input image is divided into nonoverlapping 8 × 8 blocks.Then, the 2D DWT is applied to each block to generate four subbands, LL2, LH2, HL2, and HH2.Finally, the coefficients in the LL2 subband of each DWT block are used to generate the feature image.[3]

SVM are a supervised learning approaches used in organization and reversion analysis. Analgorithm of SVM training constructs a model that can classify whether a new sample falls into which of the category the system is trained for the database.

II. LITERATURE REVIEW

Mayank vasta et. al[4] in this paper presents a newwatermarking technique of biometric image algorithm which synergistically combines the DWT and LSB based algorithms for improved robustness and resiliency when subjected to both geometric and frequency attacks. For this used a biometric mul-timodal algorithm as a metric to estimate fingerprint and face recognitioncombined performance. The outcomespresent that the pro-posed watermarking algorithm is more robust to geometric and frequency attacks compared to either the LSB or DWT based techniques. The pro-posed algorithm also safety integrity of both the face template and the fingerprint image.

Khalil et.al[5] In this paper, a robust DWT-based multibit watermarking system for fingerprint images has been proposed. The proposed system exploits the HVS characteristics and the properties of fingerprint images via a proposed perceptual model to strengthen the presence of the watermark while maintaining its imperceptibility. A maximum-likelihood decoder using the GGD model and taking into account the perceptual masking has been presented. The proposed method has been authenticated via extensive experiments, where the results have shown significant improvements over the conventional watermarking technique as well as a superiority over recent state-of-the-art algorithms in terms of robustness.

Rajlaxmi Chouhan, et al. using watermarking of fingerprint image throughused DWT. The extraction/embedding for each image in the database has been attainedeffectively and watermarking method is found to provide equally good results for all fingerprint in the database [6].

Sengul Dogan, et al. Recommend a biometric color images hiding method An Watermarking technique based on the Discrete Cosine Transform (DCT), which is used to the protect security and integrity of transmitted biometric color images [7].

Meenakshi Arya1, et al. Applied two different method, one for biometric on image of signature, additional for watermarking (SVD) to reduce a dataset including a huge number of value to a dataset containing meaningfully fewer values but which still includingbig variability fraction present in the original data [8].

Sandip Dutta, et al. In which unique key is createdapplyingjointreceiver's and sender's finger prints partial portion. From this unique key a random sequence is produced, which is utilized as an asymmetric key for both Encryption and Decryption [9]

Rajlaxmi Chouhan et al. proposed Fingerprint Authentication through Wavelet-based Digital Watermarking. The DWT based method has been found to give improvedgeometrical distortions, robustness against noises, JPEG and filtering compression attack than various frequency domain watermarking techniques. Moreover the suggested method is compared with DCT based and hybrid DWT- DCT watermarking techniques, but as a resultant the performance of the proposed technique is better than the other compared techniques[10].

R. Ashoka Rajanl.et.al [11s] The four different images of fingerprint, where every image is further isolated into 4 different quadrants and every quadrant watermarked image with the encrypted numeric digit. As four watermarked image of fingerprints with a modified ATM pin number of the same client, the proposed work discovers application in security usage in view of cryptographic unique fingerprint watermarking. Such a combination of watermarking strategies and encryption gives a level of security and further shields the client's personality from assaults because of the procedure's strength. The experimental study is complete on a limited number of clients and the outcomes show that hybrid methodology gives enhanced results as far as other existing methodologies in the literature.

III. PROPOSED METHODOLOGY

In this study, we work on fingerprint images with ATM PIN for security purpose. In the first step, take fingerprint image as an input image for steganography. Take ATM PIN to hide into image using LSB method. Encrypt ATM PIN using RSA encryption algorithm. In the second step, take stego image (hidden image) as a cover image. For memory saving, create watermark image using BCI. After, 3-level DWT for embed both images with scaling factor 0.001 and calculate the standard deviation of LL band and store features. Then extract watermark image using 3-level DWT and also apply poisson noise attack on watermarked image. Apply rotate attack

with 45° on watermarked image. Finally classify the data using MLPSVM classifier.

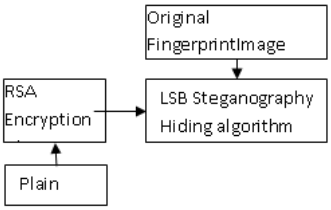


Fig. 1 Block Diagram of Steganography Process

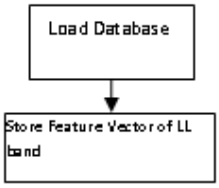


Fig. 2 Load Database and Extract Feature

Proposed Algorithm

The methodology operates on the basis of the steps below:

A. Steganography Algorithm

1) Select fingerprint image of size M*N as an input.

2) Take ATM PIN as a input text.

3) Apply RSA algorithm to encrypt and decrypt message:

a. $PK = p \times q$ (1)

b. $\emptyset = (p-1) \times (q-1)$ (2)

c. Where pk=public key, p and q are two prime numbers

4) Assume Alice needs to send Bob a bit pattern, or number, m such that m < n.

5) To encrypt the message, Alice uses Bob's public key and determines the cipher text 'c' as: c = m^e mod n

6) Calculate LSB of every pixel of red image.

7) Perform LSB on the red image to embed text into the original RGB image.

a. $LSB = mod(\big(I(i,j)\big), 2)$ (3)

b. Where LSB is the Least Significant Bit, I is Encrypted image and i, j is size of the image

8) Put back LSB of the red image with each bit of secret message one by one.

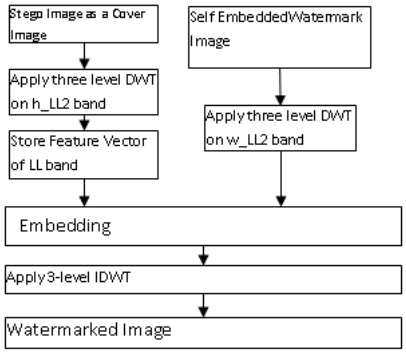


Fig. 3Block Diagram of Embedding Process

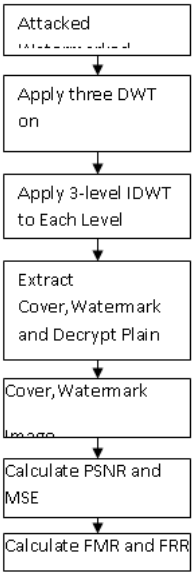


Fig. 4 Block Diagram of Extraction Process

B. Embedding Algorithm of Watermarking

1) Select a stego image as a cover image and Watermark image.

2) Obtain Watermark image using BCI method.

3) Perform 1-DWT on the stego image and also watermark image to the decompose it into four different non-overlapping multi-resolution coefficient sets: h_LL,h_LH,h_HL,h_HH and w_LL, w_LH, w_HL, w_HH

4) Apply 2-DWT to further divide h_LL and w_LL part into four bands: h_LL1, h_LH1, h_HL1, h_HH1 and w_LL1, w_LH1, w_HL1, w_HH1

5) Apply 3-DWT to further divide h_LL1 and w_LL1 part into four bands: h_LL2, h_LH2, h_HL2, h_HH2 and w_LL2, w_LH2, w_HL2, w_HH2

6) Embed image with scaling factor 0.1 and scaling factor is used to control strength of an image.

$$S_{wimgr} = h_{LL2} + (0.0001 \times w_{LL2}) \quad (4)$$

7) Perform the 3-level IDWT on the DWT transformed image, to obtain the watermarked original image on four coefficients: newhost_LL, h_LH2, h_HL2, h_HH2

C. Extraction Algorithm of Watermarking and Classification

1) To decrypt the message, Bob uses Bob's private key and determines the plain text, m as:

m = c^d mod n ; where d is decrypt , c is cipher text, m is plain text

2) Decrypt text from the watermarked image using RSA decryption algorithm.

3) Apply 3- level DWT to extract watermark image and divide watermarked image into four bands: wm_LL2, wm_LH2, wm_HL2, wm_HH2

4) Using this formula extract watermark image:

$$S\_ewatr = \frac{wm\_LL2 - h\_LL2}{0.0001} \quad (5)$$

Where wm_LL is watermarked image LL band and h_LL is cover image LL band

5) Apply Noise attack and rotate attack on watermarked image for security purpose.

6) Classify the data using MLPSVM classify between cover image and database images which contain watermarked image, noise attack image and rotate attack image.

IV. RESULT ANALYSIS

MATLABR2012a is a data analysis and visualization tool which has been designed with powerful support for matrices and matrix operations. Along with this, Matlab has excellent graphics capabilities, and its own powerful programming language. One of the reasons that Matlab has become such an important tool is through the use of sets of Matlab programs designed to support a particular task. These sets of programs are called toolboxes, and the particular toolbox of interest to us is the image processing toolbox. The experimental database contains 8 images of one person.In this research, five performance parameters have been used to demonstrate the performance of the proposed method. The two parameters are- PSNR, ACCURACY, Time, FMR and FRR.

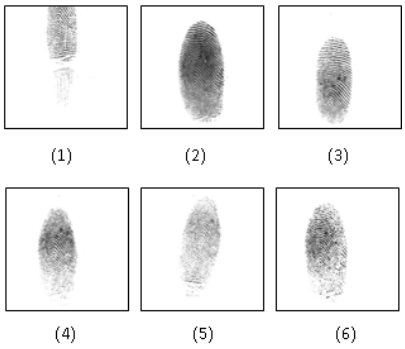


Fig. 5 Image Database of Fingerprint Images

1) Calculate Mean Square Error (MSE) value of watermarked and cover image.

$$MSE(x) = \frac{1}{N}||x - x\hat{}||^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x\hat{}2 \quad (6)$$

Where x is cover image, x^ is watermarked image, N is the size of the cover image

2) Calculate Peak Signal Noise Ratio (PSNR) value of watermarked and cover image.

$$PSNR(x) = \frac{10\ X\log((double(m).\hat{}2))}{MSE(x)} (7)$$

Where m is the maximum value of the cover image

3) False Matching Rate: It is the probability that the system will decide to permt access to an (FMR) imposter

$$FMR = \frac{False\ Matches}{Imposter\ Attempts} \quad (8)$$

The imposter attempts are implemented through matching all input image with every template images. False match was recorded for the every imposter attempt when the matching score was higher than the recognized threshold.

4) False Rejection Ratio:

$$FRR = \frac{number\ of\ falsely\ rejected\ images}{Total\ number\ of\ persons\ in\ the\ database} \quad (9)$$

*A. Read Fingerprint image as an 512*512 size.*

Fig. 6 Fingerprint Image

B. Hide ATM PIN into Image using LSB

Fig. 7 Stego Image

C. Take Stego Image as a cover image and obtain watermark image using BCI

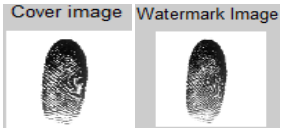


Fig. 8 Read Cover Image and Watermark Image

D. Embedding Process

Fig. 9 Watermarked Image

E. Apply Poisson Noise Attack on watermarked image

Fig. 10 Show Noise Attack,Recovered Image,Show Extracted Image

F. Apply Rotate Attack with 45° on watermarked image

Fig. 11 Show Rotate Attack,Recovered Image,Show Extracted Image

TABLE I. *COMPARISON BETWEEN BASE [4] AND PROPOSED SYSTEM*

Ratio	R. Ashoka Rajan [11]	Proposed
False Match Ratio	0.05	0.5833
False Rejection Ratio	0.761	0.7500

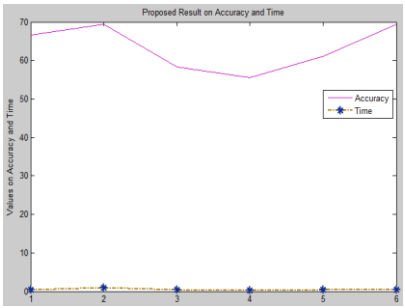
It can be seen from the Table1 that the low value of FRR and FMR are evaluated from the proposed method compared to the existing methods for all images.

TABLE II. *PROPOSED RESULTS ON PSNR ATTACK*

Image	Noise PSNR	Rotate PSNR
(1)	79.65	91.79
(2)	78.93	89.40
(3)	80.23	92.22
(4)	79.08	89.11
(5)	78.72	89.57
(6)	78.55	88.95

TABLE III. *PROPOSED RESULTS ON ACCURACYAND TIME*

Image	Accuracy	Time
(1)	66.67	0.4980
(2)	69.44	0.8720
(3)	58.33	0.5126
(4)	55.56	0.1789
(5)	61.11	0.4844
(6)	69.44	0.4990



Graph1. Shows Proposed Results

Graph1 has demonstrated the quantized examination of the Time and ACCURACY of various pictures utilizing ACCURACY (pink color), and Time (blue color) using Proposed method. This diminishing speaks to change in the target nature of the picture.

V. CONCLUSION

In this paper we worked on fingerprint images with ATM PIN for security purpose. By this technique providing security to ATM user by avoid ATM pin and use of user fingerprint as input. Watermarking their pin number after encryption in their corresponding fingerprint quadrant images helps in creating a new virtual identity for the user. The experiment result evaluated in terms of FMR,FRR, PSNR,Time and ACCURACY. The proposed result showed better accuracy FMR=0.5833 and FRR=0.7500.

VI. REFERENCES

[1] Ameya K. Nail, Raghunath S. Holambe." A blind DCT domain digital watermarking for biometric authentication." International Journal of Computer Applications (0975-8887) VOL. 1, NO. 16, 2010, pp. 11-15.

[2] Jitendra Kumar Gothwal, Ram Singh," Study of Fragile Watermarking to Protect the Fingerprint Database Template" ISSN: 2249 – 8958, Volume-3, Issue-5, June 2014,pp 250-254

[3] Wioletta Wójtowicz," A Fingerprint-Based Digital Images Watermarking for Identity Authentication",pp 85-96, DOI: 10.2478/umcsinfo-2014-0008

[4] Shang-Lin Hsieh,1 Chun-Che Chen,1,2 andWen-Shan Shen1," Combining Digital Watermarking and FingerprintingTechniques to Identify Copyrights for Color Images", Volume 2014, Article ID 454867, 14 pages

[5] Mayank Vatsa1, Richa Singh1, Afzel Noore,Max M. Houck,and Keith Morris "Robust biometric image watermarking for fingerprint and face template protection" IEICE Electronics Express, Vol.3, No.2, 23–28, 2006.

[6] Khalil Zebbiche, Fouad Khelifi "Efficient wavelet-based perceptual watermarkmasking for robust fingerprint image watermarking"The Institution of Engineering and Technology 2013.

[7] Rajlaxmi Chouhan, Agya Mishra, and Pritee Khanna, "Wavelet-based Robust Digital Watermarking Scheme for Fingerprint Authentication", Rajlaxmi Chouhan is a Master student in Electronics & Communication, Engineering at Indian Institute of Information Technology, Design & Manufacturing Jabalpur 482 005 India, 2011

[8] Sengul Dogan & Turker Tuncer & Engin Avci," A New Watermarking System Based on Discrete Cosine Transform (DCT) in Color Biometric Images", Received: 22 February 2011 / Accepted: 6 April 2011, Springer Science +Business Media, LLC 2011.

[9] Meenakshi Arya, and Rajesh Siddavatam, "A Novel Biometric Watermarking Approach Using LWT- SVD", V.V. Das, G. Thomas, and F. Lumban Gaol (Eds.): AIM 2011, CCIS 147, pp. 123–131, 2011. Springer-Verlag Berlin Heidelberg 2011.

[10] Sandip Dutta, Avijit Kar, N.C. Mahanti, and B.N. Chatterji, "a biometrics based(fingerprint) Encryption / Decryption Scheme", 2012.

[11] R. Ashoka Rajanl, R.Angelinjosphia2, Ms .PVS.Gayathd, T.Rajendran4 ,P. Anandhakumar5," A Novel Approach for Secure ATM Transactions Using Fingerprint Watermarking", 2013 Fifth International Conference on Advanced Computing (ICoAC).

