ISSN No. 0976-5697

Volume 5, No. 6, July-August 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Improved Multi-Model Biometric Authentication using Watermarking and Visual Cryptography

Aditi Verma*
M.Tech. Student, CSE Dept.
PDM College of Engineering for Women

Meha Khera
Assistant Professor in CSE Dept.
PDM College of Engineering for Women

Abstract: Information security is one of the most promising research area that confirms the secure data communication between distance users. There are number of cryptographic and steganography techniques to secure the information. In this work, a hybrid multi-model biometric architecture is presented that combines the watermarking, cryptography and biometric authentication. This multi-model architecture includes two types of biometric images i.e. iris and finger print image. This presented hybrid model is defined in three different layer where each layer defines a separate level of security. In first stage, the visual cryptography is performed by using the half tone fingerprint and iris images. This visual cryptography will use the random sequence algorithm to perform the visual cryptography. The cryptographic image will not increase the size of the image. At the second stage, this visual cryptographic image will be stored behind any source biometric object. To perform the image watermarking in other image, DWT based image will be implemented. Now this dual biometric embedded cover image will be communicated at the receiver side. On the receiver side, the reverse process of watermark recovery and the retrieval of biometric image from the cryptographic watermarked object. At the final stage, these two biometric images will be compared with the biometric image dataset to confirm the biometric authentication. To perform this authentication, the weighted PCA will be implemented. The proposed work will be implemented in matlab environment. The analysis of the work will be performed on each stage of the presented model.

Keywords: Iris, Fingerprint, Authentication, Visual Cryptography, Watermarking.

I. INTRODUCTION

Digital media processing enable the easy distribution of different kind of media. The easy distribution of digital media gives unauthentic copying or theft of digital Medias. In order to reserve the authentication rights to the content provider is done by embedding the digital objects in these multimedia data. A Watermarking object can be any image or some other digital content that contains the information about the author or the host or the content provider. Enabling the Watermarking appropriately helps to follow up the expected violation of copyrights.

Watermarking: Watermarking is a process of embedding a secret image into a cover image[1,5].

In digital media processing there are different methods to hide some secret digital information in some other media[2]. Watermarking basically hide the secret information among media files so that secret communication can be drawn between end users.[4]

A Standard Watermarking scheme adapted by any multimedia data is shown in figure 1[6,7].

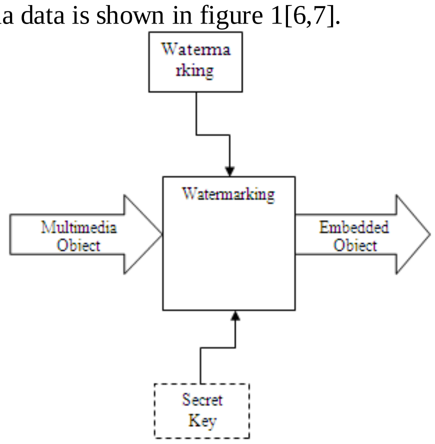

Figure 1: Basic Watermarking Process

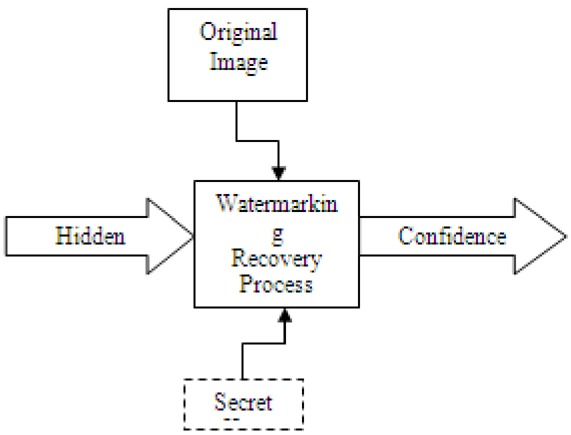

Figure 2: Watermarking Recovery Process

The recovery process from the embedded object is reversed to the Watermarking process and the Watermarking recovery model is shown in figure 2.

There are number of Watermarking approaches introduced by different authors in last 24 years.[11] These all Watermarking approaches are categorized under different vectors. The different vectors of these classifications are listed in table 1.

Table 1: Classification of Watermarking under Different Vectors

Classification Vector	Categories
Type of Inserted Media	Text, Image, Video, Audio
Robustness	Robust, Fragile, Semi-Fragile
Watermarking Object	Noise, Image
Necessary Data for Watermarking	Private, Semi-Private, Public
Processing Approaches	Bitwise, Patch Based, Randomize, Lookup Table Based, Spread Spectrum based etc.

A. *Digital Image Watermark using 'Discrete Wavelet Transform':*

DWT offers multiresolution representation of an image and DWT gives perfect reconstruction of decomposed image .Image itself is considered as two dimensional signals. When image is passed through series of low pass and high pass filters, DWT decomposes the image into sub bands of different resolutions [Ratnaparkhe et. al., 2008, Joshi et. al. 2008]. Decompositions can be done at different DWT levels. DWT offers mutiresolution representation of a signal. One Level DWT- Decomposition is given in Fig.

LL: Approximate Subband	HL: Horizontal Subband
LH: Vertical Subband	HH: Diagonal Subband

Figure 3 : One Level Image Decomposition

It has been widely accepted that maximum energy of most of natural images is concentrated in 'approximate (LL) subband' which is low frequency subband. Hence modification to the coefficients of these low frequency subbands would cause severe and unacceptable image degradation. Hence, we do not embed watermark in LL subband. The good areas for watermark embedding are high frequency sub bands (vertical, horizontal and diagonal components). The human naked eyes are not sensitive to these high frequency sub bands. So, effective watermark embedding is achieved without being perceived by human eyes. The generalized DWT based watermarking is shown in Fig..

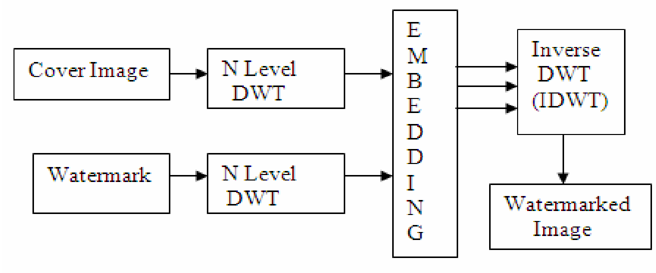

Figure 4.: Generalized DWT based Watermarking Scheme

B. *Watermarking Applications:*

a. *Content Identification:*

The main effectiveness of Watermarking is to provide the proof to the ownership and the copyrights respective to the usage monitoring and the royalty tracking for the Watermarking data so that the contents are identified and remain safe for the specific owner. The monitoring of the contents is respective to the deployment of the approach.

b. *Transaction Identification:*

The another advantage of Watermarking is in distribution management where the distrutors are assigned with the serialzed copies. So that by analyzing the owner of the order can be identified. This approach is beneficial to generate the pirated copies by using the transactional Watermarking.

c. *Asset Management:*

The Watermarking creates a persistent media asset tag.

d. *Broadcast Monitoring:*

Enables content owners and distributors to track broadcast dissemination of their content.

e. *Copyright Communication:*

Watermarking enable copyright holders to communicate their ownership and offer links to copyright and purchase information, thereby helping to protect their content from unauthorized use, enabling infringement detection and promoting licensing.

f. *Forensic Tracking:*

Forensic tracking locates the source of content, especially illegitimate content. {A unique customer identification number can be embedded into the fingerprint).

g. *Remote Triggering:*

Identifies content and causes automatic action during distribution. The Watermarking can trigger the insertion of local or regional advertisements or service announcements and it can link to unique databases at any individual sites where the Watermarking is detected thus creating endless possibilities for the functions that it may enable.

h. *Authentication:*

It helps in identifying if content has been altered.

I. *e-Commerce/Linking:*

Links content to related information, usually on the Internet. The value is that Watermarking enables the user to purchase or access information about the content, related content, or items within the content. The Watermarking payload includes the content identification, and possibly distributor identification.

J. *Filtering/Classification:*

Enables content to be identified, classified, and used appropriately. This enables users to selectively filter potentially inappropriate content, such as consumers determining what content is appropriate for their children. The Watermarking carries the content identification or classification code.

K. *Rights Management:*

Enables digital rights management (DRM) systems to connect content outside the DRM, and back to the DRM, such as linking the content to usage rules, billing information, and other critical metadata.[9]

II. VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) is a type of secret sharing scheme introduced by Naor et al. In a -out-of-n scheme of VC, a secret binary image (SI) is crypto- graphically encoded into n shares of random binary patterns. The shares are xeroxed onto n transparencies, respectively, and distributed amongst n participants, one for each participant. Every participant has its own share and no other participant show it to another participant. Participants can visually reveal the secret image by superimposing any t transparencies together. The secret cannot be decoded by any $t-1$ or less participants, even if infinite computational power is available to them. Being a type of secret sharing scheme, visual cryptography can be used in a number of applications including access control. For instance, a bank vault must be opened every day by three tellers, but for security purposes, it is desirable not to entrust any single individual with the combination. [14]

Random Sequence Algorithm is used for the process of visual cryptography. In this algorithm, A random matrix is generated which gets ORed with the binary form of the image that needs to be encrypted. The resultant binary form is again converted into the image which as a result is the encrypted image.

III. PROPOSED WORK

In this present work, a dual biometric authentication scheme is represented using iris and fingerprint impression recognition. The presented authentication model is based on the Watermarking and multi-model biometric authentication. The work is divided in three main stages. In first stage, the iris image is accepted as the cover image and to perform the data hiding over the iris image. At second stage, fingerprint impression will be used as the hidden data object. The fingerprint image is encrypted using visual cryptography. In this work, a bit sequence based ex-oring mechanism is applied for visual cryptography. The DWT is here applied to hide the encrypted fingerprint image over the iris image. [8,13] At the final stage, weighted PCA based approach is defined to perform the dual biometric authentication. At the second end, when the Watermarking image is retrieved the separation of facial image and thumb image will be performed. Now the weighted PCA will be applied to perform the biometric authentication.[16] The associated methodologies with proposed work are given here under.[3]

In this present work analysis is performed under different approaches such as MSE, PSNR, Image similarity etc. The overall research model is shown here under-

A. *Research Methodology:*

Basic Model

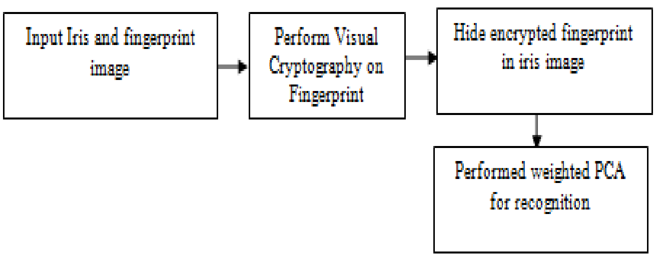

Figure 6 : Basic Model

Here figure 6 is showing the basic model used by any presented stegganography based recognition approach. As we can see, the work starts with the input in the form of Source Cover Image and Digital image or information to hide behind the image. The foremost task is to encode the input fingerprint image using visual cryptography. [15]As the region identification is done, the data hiding is performed over the image.[12] This result image then processed under the recovery algorithm to perform the decoding. After decoding on original image the hidden data will be extracted from the image. At the final stage, the analysis of work is done under different algorithms.[10]

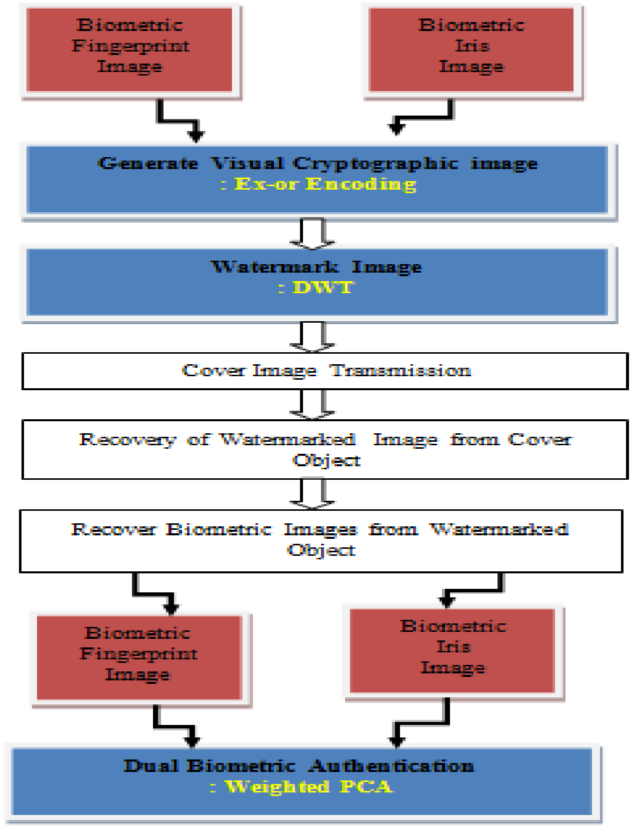

Figure 5 : Flow of Work

B. *Evaluation:*

To check the performance of the proposed technique several parameters are used. Parameters evaluate the technique in terms of hiding capacity, the error between cover image and stego image and the quality of the stego image.

C. *Need of Evaluation Parameters:*

a. To find the error between cover image and stego image.
b. To measure the quality of the stego image by comparing it with cover image.
c. To find the size of the data in cover image that can be modified without dete*riorating its integrity*.

D. *Evaluation Parameters:*

a. *Mean Square Error(MSE):*

It is defined as the square of error between cover image and stego image. The distortion in the image can be measured by MSE.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[(i,j) - K(i,j)]^2$$

Where:
I(i,j) is the value of the pixel in the cover image.
K(i,j) is the value of the pixel in the stego image.
m n:rows and columns of image(size of image).

b. *Peak Signal to Noise Ratio(PSNR):*

It is the measure of quality of the image by comparing the cover image with the stego image.

$$PSNR = 10 * \log\left(\frac{255}{MSE}\right)$$

c. The Bit Correct Ratio (BCR):

It represents the ratio of correct extracted bits to the total number of embedded bits. Some attacks are applied to the watermarked images to check for the robustness of the techniques. After every attack the BCR is computed of the extracted watermark. It is expressed using the formula:

$$BCR = \frac{100}{l}\sum_{n=0}^{l-1}\begin{cases}1, & Wn' = Wn\\ 0, & Wn' \neq Wn\end{cases}$$

$$\text{BCR} = \frac{100}{l}\sum_{n=0}^{l-1}\begin{cases}1, & Wn' = Wn\\ 0, & Wn'! = Wn\end{cases}$$

Where, l represents watermark length, W_n represents the n^{th} bit of the original watermark and W'_n represents the n^{th} bit of the recovered watermark.

d. Structural Similarity Index Measure (SSIM) :

It is the used to measure similarity between two images. Images can be either original image and watermarked image or original watermark and recovered watermark. It is designed to improve on traditional methods like PSNR and MSE. It is full reference matrix where the quality measure of image is based on an initial distortion free image as reference. Its value exit between the decimal values 1 and -1. If SSIM is equal to 1, it means the images are identical sets. It is calculated as:

$$\text{SSIM}(x. y) = \frac{(2\mu_x \mu y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma^2_x + \sigma^2_y + C_2)}$$

Where, μ_x is average of x , μ_y is average of y, σ^2_x is the variance of x, σ^2_y is the variance of y, σ_{xy} is the covariance of x & y , C_1 and C_2 are the two variable to stabilize the division with weak denominator.

E. Introduction to the Tool – Matlab:

MATLAB is a programming environment for algorithm development, data analysis, visualization, and numerical computation. Using MATLAB, we can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran.

We can use MATLAB in a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology.

IV. EXPERIMENTAL RESULTS

Figure 7 indicates the biometric image i.e. fingerprint image that is to be hidden inside the figure 8 which is the cover image i.e. iris image.

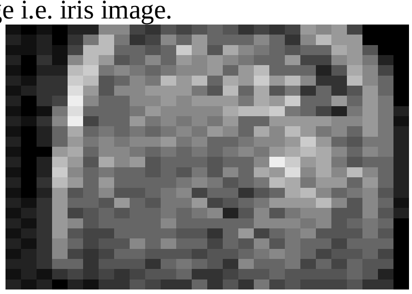

Figure 7: Fingerprint Image

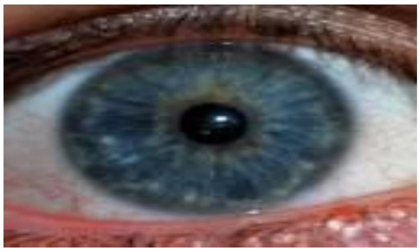

Figure 8: Iris Image

Steps to be performed are:

Step 1: Reading the fingerprint and iris images.

Step 2: Apply random sequence algorithm to perform visual cryptography on fingerprint image and the resultant image of this step is indicated as Figure 9.

Figure 9 : Encrypted Image

Step 3: Hide this encrypted image inside the cover image which is the iris image and the resultant image of this step is indicated as Figure 10.

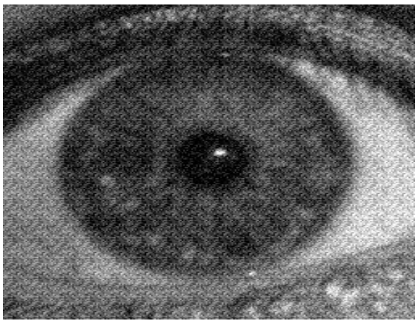

Figure 10: Watermarked Image

Step 4: Fingerprint Image is recovered from the watermarked image, marked as figure 11.

Figure 5: Recovered Image

Step 5: Error metrics PSNR and MSE are calculated in order to find out the error in original and recovered image. PSNR and MSE are calculated which comes out to be:

PSNR(Peak Signal to Noise Ratio)= 11.1737

MSE(Mean Square Error)= 4.962

Step 6: In the final step, Recovered image is being compared to the images in dataset in order to provide authentication.

V. CONCLUSION

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Watermarking can be used for hidden communication. A stego-key has been applied to the system during embedment of the message into the cover image. This Watermarking application software provided for the purpose to how to use any type of image formats to hiding any type of files inside there. In this work, a biometric authentication system is presented with steganography concept. Here the fingerprint and iris images are considered as biometric images. At the earlier stage, the visual cryptography is applied to encode the fingerprint image. Later on the DWT based approach is applied to hide the encoded fingerprint image in iris image. After this the stego-object is communicated to the receiver. As the receiver read the image, the reterival process is applied over it. After the reterival of fingerprint and iris image, the weighted PCA approach is applied for recognition. The presented work is implemented in matlab environment. The results shows the significant results in terms of data strorage and successful reterival.

Watermarking has a wide array of uses. For example, it can be used for digital watermarking, e-commerce, and the transport of sensitive data. Stegography involves embedding hidden watermarks, or identification tokens, into an image or file to show ownership. This is useful for copyrighting digital files that E-commerce allows for an interesting use of Watermarking.

Watermarking can also employ in following areas:

A. Encoding Secret Messages in Text:

B. Encoding Secret Messages in Images:

C. Encoding Secret Messages in Audio:

VI. ACKNOWLEDGEMENT

I would like to thank Abdulaziz, N.K. and Pang, K.K for their paper ‘Robust Data Hiding for Images’ published in IEEE International Conference on Communication Technology.

VII. REFERENCES

[1]. Abdulaziz, N.K. and Pang, K.K., (2000) “Robust Data Hiding for Images”, Proceedings of IEEE International Conference on Communication Technology, WCC - ICCT 2000, Vol. 1, 21-25, Aug. 2000, pp. 380 – 383.

[2]. Akram, M. Zeki, Azizah A. Manaf and Shayma S. Mahmod (2011) “High Watermarking Capacity Based on Spatial Domain Technique”, Information Technology Journal, Vol. 10, 2011, pp.1367-1373.

[3]. Alvarez, P. (2004) “Using extended file information (EXIF) file headers in digital evidence analysis”, International Journal of Digital Evidence, Economic Crime Institute (ECI), Vol. 2(3), 2004, pp. 1-5.

[4]. Amin, M.M., Salleh, M., Ibrahim, S., et al. (2003) “Information Hiding Using Watermarking”, 4th National Conference On Telecommunication Technology Proceedings (NCTT2003), Shah Alam, Malaysia, January 14-15, 2003, pp. 21-25

[5]. Anu, Rekha, Praveen (2001) “Digital image Watermarking”, International journal of computer science & informatics, volume-1, issue-ii, 2011.

[6]. Avcıbas, I., Nasir M., and Bülent S., (2003) “Steganalysis Using Image Quality Metrics”,IEEE transactions on image processing, vol. 12, 2003.

[7]. Avcibas, N. Memon, and Sankur B. (2001) “Steganalysis using image quality metrics," Security and Watermarking of Multimedia Contents, San Jose, Ca. , Feruary 2001.

[8]. Bailey, K. and Curran, K., (2006) “An evaluation of image based Watermarking methods”. Multimedia Tools and Applications, vol. 30 (1), 2006, pp. 55 – 88.

[9]. Besdok, E. (2005) “Hiding information in multispectral spatial images” Int. J. Electron. Commun. Vol. 59, 2005, p. 15 – 24.

[10]. Cachin, C. (1998) “An Information-Theoretic Model for Watermarking”, in proceeding 2nd Information Hiding Workshop, vol. 1525, 1998, pp. 306-318,

[11]. Chandramouli, R., Memon, N. (2001) “Analysis of LSB Based Image Watermarking Techniques”, IEEE, 2001. pp. 1019-1022,

[12]. Farid, H. and Lyu S. (2002) “Detecting hidden messages using higher-order statistics and support vector machines," 5th International Workshop on Information Hiding., 2002.

[13]. Fridrich, J. (2004) “Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes," Proc. 6th Information Hiding Workshop, Toronto, Canada, May 23-25, 2004.

[14]. Fridrich, J., Goljan, M., Rui, Du(2001) “Steganalysis Based on JPEG Compatibility” Center for Intelligent Systems, Department of Electrical Engineering, SUNY Binghamton, Binghamton, NY 13902-6000.

[15]. Graps, A., (1995) “An Introduction to Wavelets”, in IEEE Computer Science and engineering, vol. 2, 1995, pp. 50-59.

[16]. Hsu Rein Lien, Mohammad Abdel, (2002) “Face detection of color images”, IEEE Transection on Pattern Analysis and Machine Intellegence, vol. 24, 2002. Pp. 696-707