Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.484 – 489

RESEARCH ARTICLE

A Dual Integrated Watermarking Approach for Biometric Authentication

Neeraj

Student, M.Tech, Deptt. Of Computer Sc., Shri Baba Mastnath Engineering College, Rohtak, Haryana

Neeru159@gmail.com

Sunita

Asstt. Professor, Deptt. Of Computer Sc. & App., College, Shri Baba Mastnath Engineering College, Rohtak, Haryana

Kashisuni5@gmail.com

Abstract— To improve the information authentication and network security one of the effective authentication mechanism is Biometric authentication System. But when this authentication system is a offline authentication system, in such case, it is required to secure this authentication information. In this work, a biometric watermarking based authentication system is defined to secure the authentication system. In this work, biometric thumb image is watermarked in facial image to provide the security to biometric authentication system. The obtained results provided by the system ensure the effective system integrity and reliability.

Keywords— Watermarking, Biometric, Thumb Impression, Security, Integrity

I. INTRODUCTION

Watermarking means, literally, covered writing. Watermarking is the art and science of hiding information such that its presence cannot be detected and a communication is happening. Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, Watermarking can be used to carry out hidden exchanges. The main goal of Watermarking is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [10]. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists

A) Watermarking Applications

There are many applications for digital Watermarking of image, including copyright protection, feature tagging, and secret communication [1,2]. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark. In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an image. Copying the stego–image also copies of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. On the other hand, secret communication does not advertise a covert communication by using Watermarking. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people

B) Steganographic Techniques

Over the past few years, numerous Watermarking techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible.

Common approaches are include:
(i) Least significant bit insertion (LSB)
(ii) Masking and filtering
(iii) Algorithm and Transform

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works good for image, audio and video Watermarking. To the human eye, the resulting image will look identical to the cover object

Masking and filtering techniques are mostly used on 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected.

In addition to DCT, images can be processed with fast Fourier transform (FFT). FFT is "an algorithm for computing the Fourier transform of a set of discrete data values". The FFT expresses a finite set of data points in terms of its component frequencies. It also solves the identical inverse problem of reconstructing a signal from the frequency data.

C) Watermark Recovery

It is not enough if a Watermarking is imperceptible. The prime concern is about (statistical) undetectability. Only a naive watermark hides messages "invisibly". A good watermark is undetectable or at least very hard to detect by any means provided the original cover is not known.

The more difficult task is providing metrics for perceptibility and robustness. Criterions suggested for the evaluation of perceptibility as shown in Table 1.

Level of Assurance	Criteria
Low	- Peak Signal-to-Noise Ratio (PSNR) - Slightly perceptible but not annoying
Moderate	- Metric Based on perceptual model - Not perceptible using mass market equipment
Moderate High	- Not perceptible in comparison with original under studio conditions
High	- Survives evaluation by large panel of persons under the strictest of conditions.

Table 1 - Summery of Possible Perceptibility Assurance Levels

- Signal enhancement (Sharpening, Contrast enhancement)
- Additive Multicative Noise (Gaussian, Uniform etc.)
- Filtering (High Pass, Low Pass, Linear etc.)
- Lossy Compression (JPEG etc)
- Geometric Transformation(Translation, Rotation) etc

II. Literature Survey

Watermarking is a branch of information hiding. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) to hide the existence of the message. Watermarking is often used in secrete communication. In recent years, many successful Watermarking methods have been proposed. Among all the methods, LSB (least significant bit) replacing method is widely used due to its simplicity and large capacity. The majority of LSB Watermarking algorithms embed messages in spatial domain, such as BPCS[10, 17], PVD[16, 18]. Some others, such as Jsteg[7, 1], F5[13] Outguess[14, 4], embed messages in DCT frequency domain (i.e. JPEG images). In the LSB Watermarking, secret message is converted into binary string. Then the least significant bit-plane is replaced by the binary string. The LSB embedding achieves good balance between the payload capacity and visual quality. However, the LSB replacing method flips one half of the least-significant bits. Thus the artifacts in the statistics of the image are easy to be detected[15].

Steganalysis is the method to reveal the hidden messages, even some doubtful media. The attacks on LSB replacing methods are most based on Chi-square analysis[12] and
the relationship of pixels or bit–planes[3]. In the frequency domain, there are some steganalysis algorithms based on histogram and block effect[5]. Among the methods, the RS steganalysis[3], proposed by Fridrich, is considered as the most reliable and accurate method to the LSB–replacing Watermarking. It utilizes the regular and singular groups as the statistics to measure the relationship of pixels. In most nature images, strong correlation exists in adjacent pixels. After the LSB–replacing Watermarking, the correlation is decreased. Thus, the proportion between the regular and singular groups changes and the existence of the Watermarking is detected. Moreover, the secrete message length can be estimated by the amount of regular and singular groups.

To resist to RS analysis, the influence on the correlation of pixels needs to be compensated. The compensation may be achieved by adjusting other bit planes. Nevertheless, the implementation may be computational infeasible. For example, if only two bit planes are modified in a 256 × 256 gray level image, there are 22 possible bit selections for each pixel. For the entire image, there are 2524288 times of adjustments. It is not feasible in the practical application. For this reason, optimization algorithms have been employed in information hiding to find the optimal embedding positions. For example**,** genetic algorithm was been exploited in digital watermarking[8, 2, 9].

Watermarking, in contrast attempts to prevent an unintended recipient from suspecting that the data is there. [14].Combining encryption with Watermarking allows for a better private communication. The goal of Watermarking is to avoid drawing suspicion to the transmission of the secret message.

III. Proposed Approach

Image information System basically deals with hiding the some information in the image itself. It gives the easy information access and the communication with the image itself. It also secures the information from the accidental as well as the intentional modification. The presented work is associated provide secure authentication to the system. The presented work is defined on provide the graphical information authentication using biometric image. This work will provide two main benefits to provide the information security based authentication. In this work, the dual authentication will be achieved by using two biometric components called facial image and the thumb image. The work will be divided in three main stages. At the earlier stage, the facial features will be extracted from image using Bacterial Foraging algorithm. The extraction will be here done in terms of high intensity points. Once the facial features will be extracted, the next work is to perform the biometric information hiding in these feature points. To perform this hiding, DCT based approach will be used. The biometric information considered here can be a thumb or the fingerprint image. Once the information is stored behind the image and the next work is to perform the information authentication at two levels. To perform the authentication using multi model biometric, weighted PCA approach will be used.
In this present work, a dual biometric authentication scheme is represented using facial and thumb 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 facial image is accepted as the cover image and to perform the data hiding

over the facial features. The feature extraction is here defined using BFO approach. The feature extraction is here in terms of pixel intensity based analysis. Once the facial features will be extracted, it will work as the cover pixel set to hide data over the image.

At second stage, Thumb impression will be used as the hidden data object. DCT is here applied to hide the thumb image over the facial image features. At the final stage, 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 PCA will be applied to perform the biometric authentication. The associated methodologies with proposed work are given here under.

In this present work analysis is performed under different approaches such as MSE, PSNR, Image similarity etc. The work also includes the analysis of approach under different attacks. The basic watermarking model is shown here under

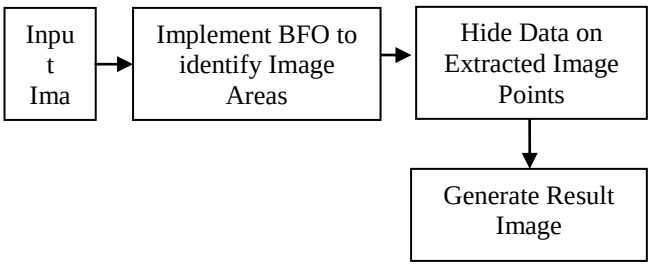

Figure 1 : Proposed Model

A) BFO

Bacteria Foraging Optimization technique is a population oriented algorithm to search optimal solutions. In this research each pixel of image is considered as the bacteria and the color of pixel is considered as the food of bacteria. The aim of the proposed algorithm will be to minimize the food source, i.e. to reduce the number of colors in the image. In the present work all the pixels of image are initially having some color, and the objective will be to optimize those colors so that the result could be investigated, that is any kind of data hidden in the image. All the colors in the image will be evaluated as the number of pixels having that color. This evaluation will define the heath status of all kind of colors which are in the image. After which depending on the health status the colors will be divided into two categories popular colors or the unpopular colors. If the health status of a particular color comes to be high then that color is present on too many pixels and will be known as popular one and all the colors with low health status will be considered as the unpopular ones.

Here, taking into consideration a stegnographed picture, which is under the R.G.B. model. And the image can be in true colour (24 bits) or in scale of grey (256 ranges of grey). The selection of the image is made on the basis of its dimensions as we are considering images with similar height and width. This algorithm is specifically for RGB model images. And it is not only detecting but also extracting the hidden text in the image.

IV. RESULTS

In this present work, a secure biometric authentication scheme is presented to provide the secure transmission of biometric object. The work is implemented in matlab environment. The results obtained from the work are described here under

The Mean Square Error(MSE), BCR(Bit Correct Ratio) and the Peak Signal to Noise Ratio(PSNR) , Similarity Ratio and Correlation of different stego images with payload facial images is shown in the table 5.1. If we compare the PSNR of all the stego images, we can say that using Boat as a cover image gives the best PSNR. The same is true in the case if we compare the MSE of different stego images. Boat as cover image gives the least MSE.

Table 2 : Analysis Parameters

Cover Image (256x256)	**Payload (50x20)**	**MSE**	**PSNR**	**Similarity**	**Correlation**	**BCR**
face1.jpg	Thumb.bmp	49.1362	31.2168	0.4721	0.9832	0.1517
face 2.jpg	Thumb.bmp	31.2375	33.1840	0.6995	0.9959	0.1275

face3.jpg	Thumb.bmp	30.4333	33.2973	0.6810	0.9953	0.1150
Face4.jpg	Thumb.bmp	30.5768	33.2769	0.5874	0.9944	0.1270
Face5.jpg	Thumb.bmp	30.2942	33.3172	0.6622	0.9945	0.1164
Face6.jpg	Thumb.bmp	30.4298	33.2978	0.5513	0.9927	0.1062

The results obtained from the work are shown in the form of graph.

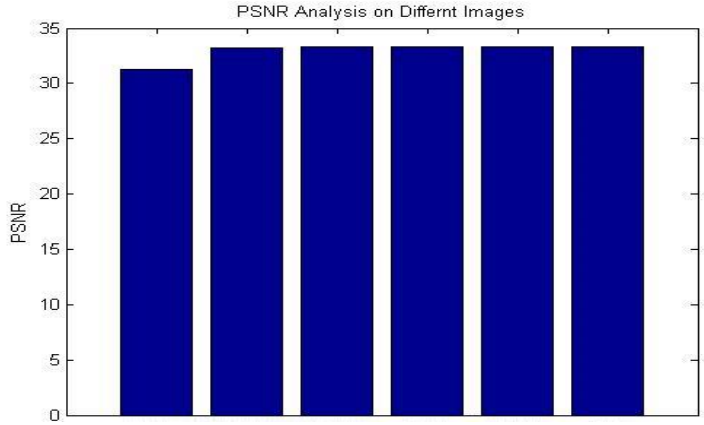

Figure 2 : PSNR Analysis on Different Images

Here figure 2 is showing the analysis of presented work under PSNR parameter. Higher the PSNR value more effective the results will be. As we can see, the presented work has provided the PSNR over 30. The obtained PSNR value is satisfactory respective to defined approach.

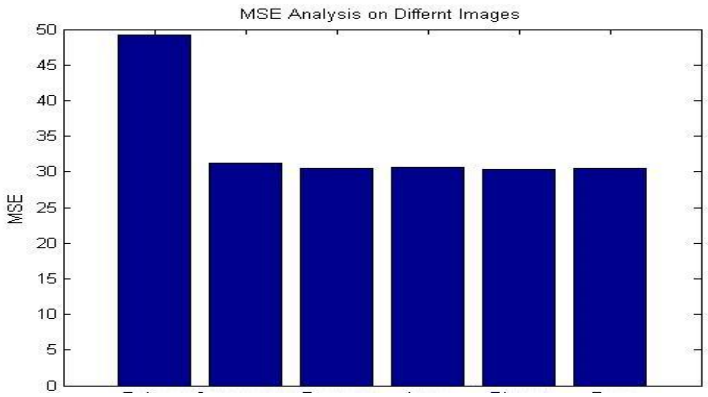

Figure 3 : Similarity Analysis on Different Images

Here figure 3 is showing the analysis of presented work under Similarity Analysis. As the stegno image is been changed because of presented work. The differences in the source and the result image are shown. As we can see, the presented work has provided the similarity ratio over 50%. The obtained Similarity ratio value is satisfactory respective to defined approach.

V. CONCLUSION

In this paper, an effective biometric authentication system is defined along with biometric watermarking scheme. The work is defined by using the BFO based pattern extraction and to perform the PCA based authentication.

REFERENCES

[1] Watermarking software for windows. http://members.tripod.com/Watermarking/stego/software.html.

[2] S. C. Chu, H. C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh. Genetic watermarking for zerotree-based applications. Circuits, Systems, and Signal Processing, 27(2):171–182, 2008.

[3] J. Fridrich, M. Goljan, and R. Du. Detecting lsb Watermarking in color, and gray-scale images. IEEE MultiMedia, pages 22–28, 2001.

[4] J. Fridrich, M. Goljan, and D. Hogea. Attacking the outguess. In Proc.ACM Workshop Multimedia and Security, 2002.

[5] J. Fridrich, M. Goljan, and D. Hogea. Steganalysis of jpeg images: Breaking the f5 algorithm. In Proc. of the ACM Workshop on Multimedia and Security 2002, 2002.

[6] D. E. Goldberg. The genetic algorithms in search, optimization and machine learning. Addison-Wesley, 1989.

[7] C. T. Hsu, J.Wu, and L. Hidden. Digital watermarks in images. Image Processing,IEEE Transactions on, pages 58–68, 1999.

[8] H. C. Huang, C. M. Chu, and J. S. Pan. The optimized copyright protection system with genetic watermarking. Soft Computing, 13(4):333–343, 2009.

[9] H. C. Huang, J. S. Pan, Y. H. Huang, F. H. Wang, and K. C. Huang. Progressive watermarking techniques using genetic algorithms. Circuits, Systems, and Signal Processing, 26(5):671–687, 2007.

[10] E. Kawaguchi and R. O. Eason. Principle and application of bpcs-Watermarking. In Proceedings of SPIE:Multimedia Systems and Applications, pages 464–472, 1998.

[11] A. R. S. Marcal and P. R. Pereira. A Watermarking method for digital images robust to rs steganal-ysis. Lecture Notes in Computer Science, pages 1192–1199, 2005.

[12] N. Provos. Watermarking detection with stegdetect. http://www.outguess.org/detection.php.

[13] A. Westfeld. F5-a Watermarking algorithm. In 4th International Workshop on Information Hiding, Lecture Notes in Computer Science,2137.Springer-Verlag, pages 289–302, 2001.

[14] A. Westfeld and A. Pfitzmann. Attacks on Watermarking systems. In Proceeding of Information Hiding-Third International Workshop, 1999.

[15] A. Westfeld and A. Pfitzmann. Attacks on Watermarking systems. Lecture Notes in Computer Science, pages 61–76, 1999.

[16] D. C. Wu and W. H. Tsai. A Watermarking method for images by pixel-value differencing. Pattern Recognition Letters, pages 1613–1626, 2003.

[17] X. Zhang and S. Z. Wang. Statistical analysis against spatial bpcs Watermarking. Computer-Aided Design & Computer Graphics, pages 395–406, 2003.

[18] X. Zhang and S. Z. Wang. Vulnerability of pixel-value differencing Watermarking to histogram analysis and modification for enhanced security. Pattern Recognition Letters, pages 331–339, 2004.

