ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Approach to Enhance Security of Biometric System Using LSB Watermarking

Komal
Research Scholar (M.Tech)
Department Of Computer Science and Applications
Kurukshetra University, Kurukshetra, India

Dr.Chander Kant
Assistant Professor
Department Of Computer Science and Applications
Kurukshetra University, Kurukshetra, India

Abstract: Nowadays there is a need to build secure methods for legal distribution of content over internet. Content can be any multimedia such as video, audio, images which are available for transmission over internet. To provide protection against unauthorized copy and distribution of this content, digital watermarking techniques are used in combination with biometrics such as fingerprint, speech and iris which are unique to an individual and are not easy to alter/replace. Previously several other techniques such as DCT, DWT are used in the same context for biometric watermarking. In this paper with the vision of enhancing the security of biometric template over some insecure network, a secure and more robust LSB watermarking scheme is proposed. It is used for embedding the biometric traits into the image in different bit planes. The proposed framework is implemented using MATLAB software.

Keywords: Biometrics, Spatial Domain, Least Significant Bit,Biometric Watermarking, Bit Plane.

I. INTRODUCTION

Biometric recognition is a well-known research field that aims to provide more efficient solutions to the ever-growing human need for security. Biometrics[1] refers to one or more intrinsic physical or behavioural characteristics which uniquely identify individuals. This identification involves one-to-many matching across large shared database which further provide a convenient authentication services for many applications including information security, physical access, financial services etc. But the multiple uses of biometric databases raises a serious issue with respect to personal privacy because biometric template having personal information could be used for unauthorized purposed. Unlike a PIN or password, a biometric template cannot be changed, recovered, or reissued if it is hacked or misused.

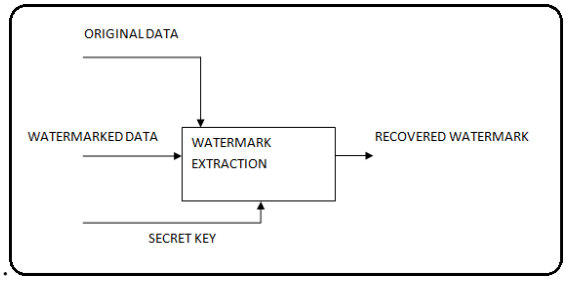


Fig 1: A Simple Diagram of Watermarking System.

Hence in order to achieve the biometric data security and secrecy, watermarking comes into play. Several schemes related to watermarking are proposed for the biometric data security one of which we shall be discussing in this paper. A simple block diagram of watermarking system is shown in Fig 1 comprising of two main steps i.e. watermark encoding and decoding.

Recently biometrics is merged with watermarking technology in order to enhance the security of multimedia content. Biometric watermarking forms a special module of digital watermarking in which the watermark content is biometric data. Access control or authenticity of legitimate user can be verified by both digital watermarking as well as by biometric authentication [2]. The ability of the biometrics technology to differentiate between an authorized person and malicious users who fraudulently acquires the access privilege of an authorized person is one of the main reasons for its popularity.

The main reason for using fingerprint template is that out of different available biometric techniques such as face, voice, fingerprint, iris, etc., fingerprint-based techniques are the most commonly used technique. So by combining watermarking with biometric features, it is easy to develop more secured and confidential watermarking techniques for providing authenticity of multimedia content because as biometric features are unique for each individual.

II. ATTACKS IN BIOMETRIC SYSTEM

In spite their number of advantages, Biometric systems are vulnerable to attacks, which lead to decrease in their security. Researcher analysed these different types of attacks that occurs and grouped them into eight classes [3]. Fig. 2 shows these attacks along with thecomponents of a typical biometric system that can be compromised.

1. Fake the biometric feature of a genuine user at the sensor (e.g. fake finger or printed face image)

2. The transmission between sensor and feature extractor may be intercepted and resubmitted by changed or replayed data

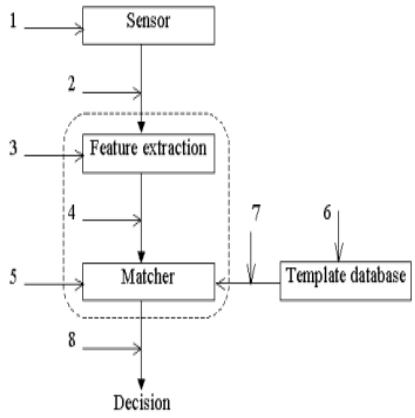


Fig 2: Eight Different Attack Points in a Biometric Authentication System

3. Override the feature extractor to produce predefined feature sets

4. Intercept and replace the extracted feature sets by a synthetic or spoofed one

5. Override the matcher so that always high matching scores are obtained.

6. Modify, replace, remove stored ore add new templates at the database

7. Intercept the communication channel between template database and matcher

8. Override the final decision

Out of these eight types of attacks, Encryption techniques have been suggested to secure the communication channels between sensor and the feature extractor, data before being submitted to matcher and last one is between database and the matcher.Hence Watermarking in combination with the biometric templates is supposed to be possible mean in enhancing the biometric system.

III. BIOMETRIC WATERMARKING

The category employs biometrics as the watermark, whereas the cover image can be any copyrighted documents. Since biometrics provides uniqueness which can't be misplaced or shared, biometric watermarking promises security against fake watermark. Fig 3 below shows a simple biometric watermarking technique.

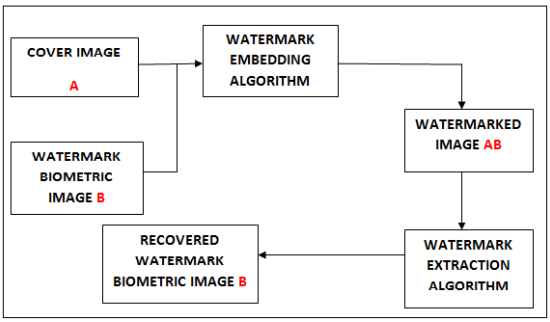


Fig 3: Biometric Watermarking

The goal of watermarking is not to improve any biometric system, but to use biometric templates as "message" to be embedded in classical robust watermarking applications such as copyright protection in order to enable biometric recognition after the extraction of the watermark. The most famous example is the "secure digital camera" where an iris template of the photographer is embedded into digital images. .

Characteristics of Biometric Watermarking

There are many characteristics that watermarking holds, some of them are as follows:

1) ***Invisibility***: An embedded watermark is not visible.
2) ***Robustness***: Piracy attack or image processing should not affect the embedded watermark.
3) ***Readability***: A watermark should convey as much information as possible.
4) ***Security***: A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties.

IV. RELATED WORK

Vatsa et al.[4] presents a novel biometric watermarking approach which embeds face image of user in to his/her fingerprint image while using DWT and Support Vector Machine based learning algorithm. They claimed that approach enhances quality, improves recognition accuracy.

Moon et al.[5] worked on multimodal biometric system employing both fingerprint and face for performance analysis on watermarking technique. Yeung and Pankanti [6] proposed an invisible fragile watermarking technique for image verification on fingerprint-based personal recognition and authentication system. To improve the security, the original watermark image is first transformed into other mixed image which does not have the meaningful appearance and this mixed image is used for new watermark image. So this algorithm is more secure.

Zebbiche et al. [7] proposed robust fingerprint watermark schema, embedding watermark data into the region of

interest of fingerprint image by using segmentation technique. DCT and DWT transform coefficients are modelled by a generalized Gaussian model. This technique ensures resiliency towards filtering, noise, and compression, cropping attacks.

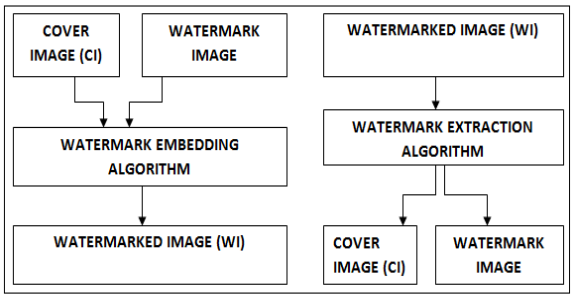
V. PROPOSED FRAMEWORK

When the image with the secret data is transmitted over the internet, unauthorized parties try to hack the data hidden over the image or change it. If the originality of the image has been altered, then it will be easier to hack the information by unauthorized persons. For improving the security, the biometric watermarks are inserted as transformed signal into the source data.

The best known Watermarking method which works in the spatial domain is the Least Significant Bit (LSB). The reason being, as we make change to MSB(Most Significant Bit) our image will start distorting giving rise to poor picture quality while in contrastmaking changes to LSB,distortion is relativelynegligible and hence cannot be seen by human eye making it the best method for watermarking.

The approach is to implement the Biometric Watermarking i.e.embeddinganbiometric template into another image without actually making any visible changes in the image. This is done using the Least Significant Bit Modification in MATLAB. The fingerprint used for watermarking in the study is taken from FVC2004 database.

(1) PROPOSED ALGORITHM



(2) PROPOSED FLOWCHART

The approach of embedding a watermark is simple and effective. The reason behind taking a grayscale bitmap image, which is 8- bit is that first there is need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a grayscale image each pixel is represented by 1bytei.e 8 bit which represent 256 gray colours between the black and white(0-255). The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side.When the data is encoded only to the last two significant bits of each colour component, there are very little chances of data being detectable because of human retina limitation in viewing such pictures.Flowchart for Watermark insertion and extraction is shown in fig 4 (i) and 4(ii).

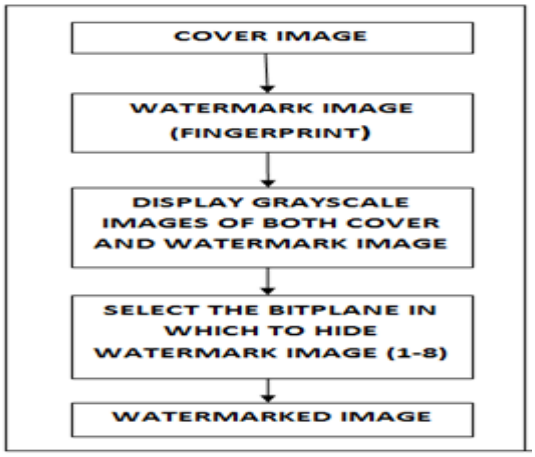


Fig 4(i): Watermark Embedding Algorithm

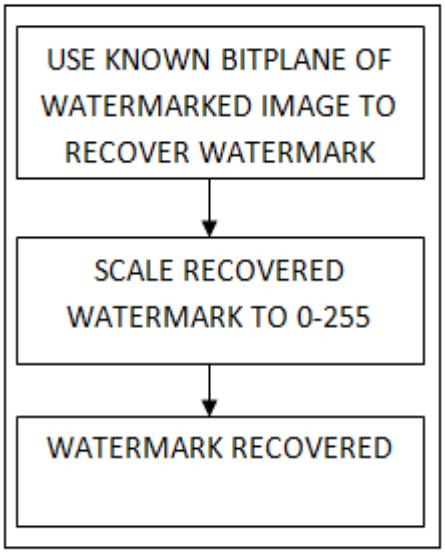


Fig 4(ii): Watermark Extraction Algorithm

VI. RESULTS

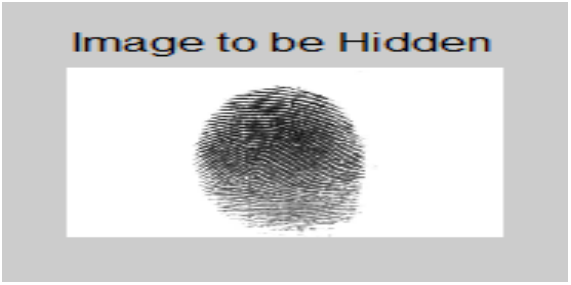


Fig 5(i): Watermark Image

Fig 5(ii): Cover Image

Fig 5(iii): Gray Scale Image Of Watermark Image(0-255)

FOR BIT PLANE 1:

Fig 5(iv): Final WatermarkedImage

Fig 5(v): Watermarked Recovered

FOR BIT PLANE 8:

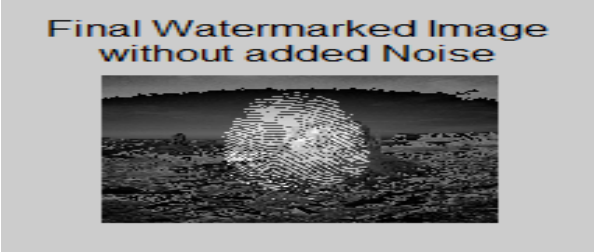


Fig 6(i): Watermarked Image

Fig 6(ii): Watermark Recovered

The results for bit plane 1 and 8 are shown in figures above. Watermark is embedded into original image using LSB algorithm, which uses the fingerprint as watermark and spreads it out to same size image. The watermarked image shows slight but unnoticeable degradation as in fig 5(iv), while the watermark (fingerprint) was recovered perfectly as in fig 5(v). In contrast as we move from LSB to MSB distortion can be seen in the cover image fig 6(i) making the picture quality poor hence it is advisable to make changes only to LSB maintaining the watermark as well as picture quality.In this way a biometric watermark is being embedded in the image data by changing only the LSB of the image data

VII. CONCLUSION

The paper studiesthe attacks and methods of biometric watermarking and evaluates LSB based watermarking scheme with different bit substitution from LSB to MSB in image. When we embed our biometric trait in the first bit i.e. LSB in the image we got watermarked image with very little distortion. Butas soon as we started embedding the data in the consequent bits i.e. second towards last MSB bit, the image starts getting distorted**..** More deep investigations are required in this field toidentify sensible application scenarios for watermarking in biometrics.

VIII.REFERENCES

[1] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, Berlin, Germany, 2003.

[2] V. ANITHA, R. V. (2012). Authentication of Digital Documents Using Secret Key Biometric Watermarking. International Journal of Communication Network Security,Vol. 1, Issue-4 .

[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, “An analysis of minutiae matching strength”, Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

[4] Vatsa, Mayank, Richa Singh, and AfzelNoore. "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking."IEICE Electron. Express 2, no. 12 (2005): 362-367.

[5] Moon, Daesung, Taehae Kim, SeungHwan Jung, Yongwha Chung, Kiyoung Moon, DosungAhn, and Sang-Kyoon Kim. "Performance evaluation of watermarking techniques for secure multimodal biometric systems." In Computational

Intelligence and Security, pp. 635-642. Springer Berlin Heidelberg, 2005.

[6] Pankanti, Sharath and Minerva M. Yeung. "Verification watermarks on fingerprint recognition and retrieval." In Electronic Imaging'99, pp. 66-78.International Society for Optics and Photonics, 1999.

[7] Zebbiche, K., F. Khelifi, and A. Bouridane. "An efficient watermarking technique for the protection of fingerprint images." EURASIP journal on information security 2008 (2008): 4.