# Applying Information Hiding into Fingerprint Verification System using Fragile Watermarking Technique

**Jitendra Kumar Gothwal, Ram Singh**

***Abstract— Protection of biometric data & templates is gaining interest and crucial issue for the security of biometric systems. Digital media in these recent days has led to an increase of digital piracy and tampering especially for biometric identification system. Digital watermarking techniques are used to authenticate a source that has been subjected to potential tempering attacks. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. Thus a protective scheme is needed which will preserve fidelity and prevent alterations. This research work had proposed an architectural framework that will apply information hiding method into biometric identification system. A Fragile image watermarking technique has been used to hide additional information into fingerprint images by changing the least significant bit value of a random chosen pixel of the image. The embedded information can be extracted without referencing to the original image. This proposed framework is to be applied in the real environment to authenticate the digital images in the database of fingerprint biometric system so that they can secured from any unwanted attacks such as intention to fraud fingerprint template. The results show that the fingerprint images are not being affected when the watermarking method is implemented and the performance of the fingerprint authentication system is also not affected when the watermarked fingerprint images are used in the system. This study can be use for image authentication especially to detect whether the image has been tampered by image processing such as noise addition and blurring***

***Keywords— Biometrics, Fingerprint, Information hiding, Fragile watermarking, Authentication systems.***

## I. INTRODUCTION

Biometrics comes from the Greek words bios (Life) and metricos (Measure) [1]. It is basically a pattern-recognition system that is used to identify or verify users based on his on her unique physical characteristics. The rapid development of digital information has also generated several new opportunities for innovation and has enabled the consumer to create, manipulate and enjoy multimedia data without any restriction. Despite the rapid growth of the digital information domain, the security and fair use of the multimedia data, as well as fast delivery of the multimedia content to a variety of end users or devices are important and yet challenging topics. Digital images had been widely used in various fields and areas. The worries of threats and attacks that could be performed to digital images could decrease the integrity and reliability of the digital data. Biometrics offers greater security and convenience than traditional identity authentication systems (based on passwords and cryptographic keys) since biometrics characteristics are inherently associated with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. A critical problem in a biometric system itself is to ensure the security of the unique biometric data, because once the biometric templates are compromised, the whole authentication system is compromised. Therefore, how to protect the biometric templates in the database and to secure transmission of the biometric templates through the open network is a vital security issue in biometrics. Numerous efforts have been made in developing effective methods in these areas in order to achieve an enhanced level of information security. There are two paramount issues in information security enhancement. One is to protect the user possession and control the access to information by authenticating an individual's identity. The other is to ensure the privacy and integrity of information and to secure information communication. Biometrics, cryptography and data hiding provide solutions to the above two issues from different perspectives [2]. Data hiding is aiming at private information protection, securing information transmission and digital rights authentication. Besides using some encryption algorithms to encode the biometric data for protection, one of the major reasons to take advantages of data hiding for biometric template protection is because data hiding complements cryptography in secret information communication and integrity authentication. The most general scenario for the information hiding is shown as the following figure 1.

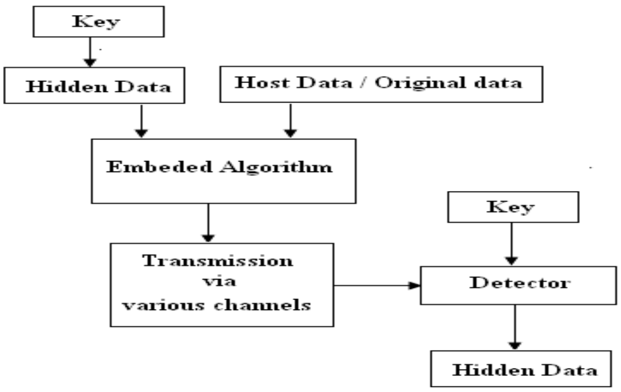

**Figure 1: Scenario of Information hiding**

**Manuscript Received on June 19, 2014.**

**Jitendra Kumar Gothwal**, Research Scholar , Department of Computer Science & Engineering, Sunrise University, Alwar (Rajasthan) ,India.

**Dr. Ram Singh**, Supervisor, Department of Computer Science & Engineering, Sunrise University, Alwar (Rajasthan), India.

## II. BIOMETRIC SYSTEM

Biometric recognition refers to the use of distinctive physiological (fingerprint, face, retina, hand geometry, iris etc.) and behavioural (voice, gait, signature etc.) characteristics, called biometric identifiers or simply biometrics. A reliable identification system is a critical component in several applications that contribute their services specifically to genuine users. Examples of such applications include physical access control to a secure facility, e-commerce, access to computer networks, attendance mark etc. Traditional methods of establishing a person’s identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms. These representations of the identity can easily be lost, shared or tolen as stated by [5]. Therefore, they are not sufficient for identity verification in the modern day world.

One of the main reasons for this popularity is the ability of the biometric technology to differentiate between an authorized person and an imposter who fraudulently acquires the access privileges of an authorized person. Biometric identification system can be more convenient for the users since there is no password to be forgotten or key to be lost and single biometric trait(e.g. fingerprint) an be used to access several accounts without the burden of remembering passwords. But while biometric techniques are offer reliable method for personal identification, the problem of security and integrity of the biometrics data poses the new issues.

For example, one personal biometric data (fingerprint template, or fingerprint features) is stolen, it is not possible to replace it as compared to a stolen identification card (ID), credit card or password [7]. Fingerprint biometric system, the technology that automatically identify individuals based on their fingerprint characteristic has been increasingly applied for positive verification process since they cannot be misplaced or forgotten and they also represents a tangible component that will identify a person's identity. In Figure 2, below shows the general framework of fingerprint biometric system. In general, biometric verification consists of two stages (Figure2): (i) Enrollment and (ii) Authentication. During enrollment, the biometrics of the user is captured and the extracted features (template) are stored in the database. During authentication, the biometrics of the user is captured again and the extracted features are compared with the ones already existing in the database to determine a match. The specific record to fetch from the database is determined using the claimed identity of the user. The fingerprint representation that has already being extracted then is matched against the fingerprint representation previously stored in the system's database either to determine or verify the identity of one person.

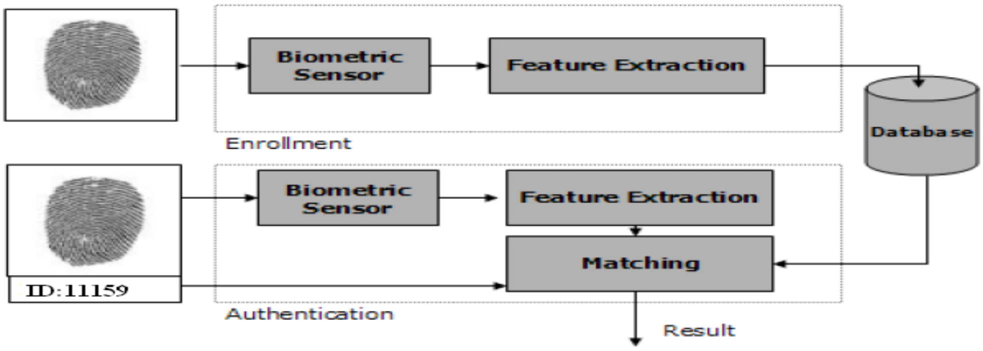

**Figure 2: General framework of fingerprint biometric system**

While fingerprint biometric system can help to authenticate one person's identity, there are still some weak points of the system that are vulnerable to attacks, which can decrease the security of the system. The attacks on fingerprint biometric system can be categorized into eight classes [11] [15]. The attacks are shown in the Figure 3, below along with the components of a typical biometric system. One of them is attack on the template database (attack number 6 on Figure 3).The unwanted user may modify or remove the existing template and also may add the new fingerprint image templates if they manage to infiltrate the database.

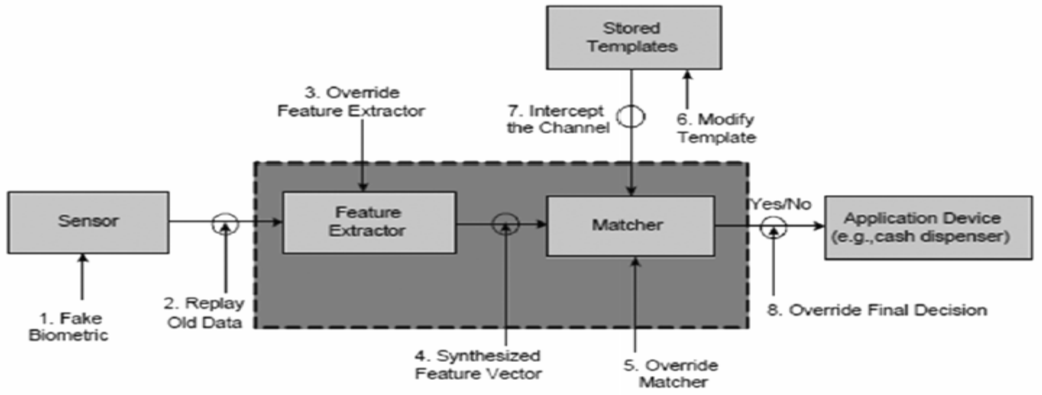

**Figure 3: Vulnerabilities in a Biometric System**

In order to promote the wide spread utilization of biometric techniques, an increased security of biometric data, especially fingerprint images, seems to be necessary. One possible solution to gratify this problem  is by using fragile image watermarking techniques which is one of the sub disciplines of watermarking  techniques is information Hiding domain. Watermarks have long been used for authentication and to prevent fraud and forgery. This technique will detect whether the Biometric data had been altered or not and also can detect the originality of the data by retrieving back the watermark data from the Biometric data. For Biometric applications many researchers are not as interested in visible watermarks as invisible watermarks. Invisible watermarks, as the name indicates, do not appear visually affect the data that they are embedded in .This method is desired if one does not want to perceptually alter the image. In this paper, we had proposed one of the information hiding techniques which is called fragile watermarking techniques that will embed a secondary data into the fingerprint images to cater the vulnerability of the images. In this way, the authenticity of the fingerprint images can be established.

## III. PROPOSED METHOD

This research has proposed an architectural framework that will help to counter the vulnerability of the fingerprint images in the database of fingerprint verification system from attack such as image tampering by unauthorized individual. This architectural framework is the modification of the existed model of fingerprint verification system. The typical system is proposed to be combined with an information hiding technique in order to enhance the security of the fingerprint images stored in the database. This research is proposing to apply a fragile image watermarking technique into the general model of fingerprint verification system in order to enhance the security of the fingerprint templates in the database The bottom part of figure shown is the proposed fragile image watermarking technique applied into the typical verification system. This frame work has been divided into four phases which are fingerprint enrollment process, watermark encoding process, watermark decoding process and fingerprint verification process. The whole process of the proposed framework can be seen in Figure 4 and the framework of embedding and detecting fragile image watermarking is similar as the other watermarking system.

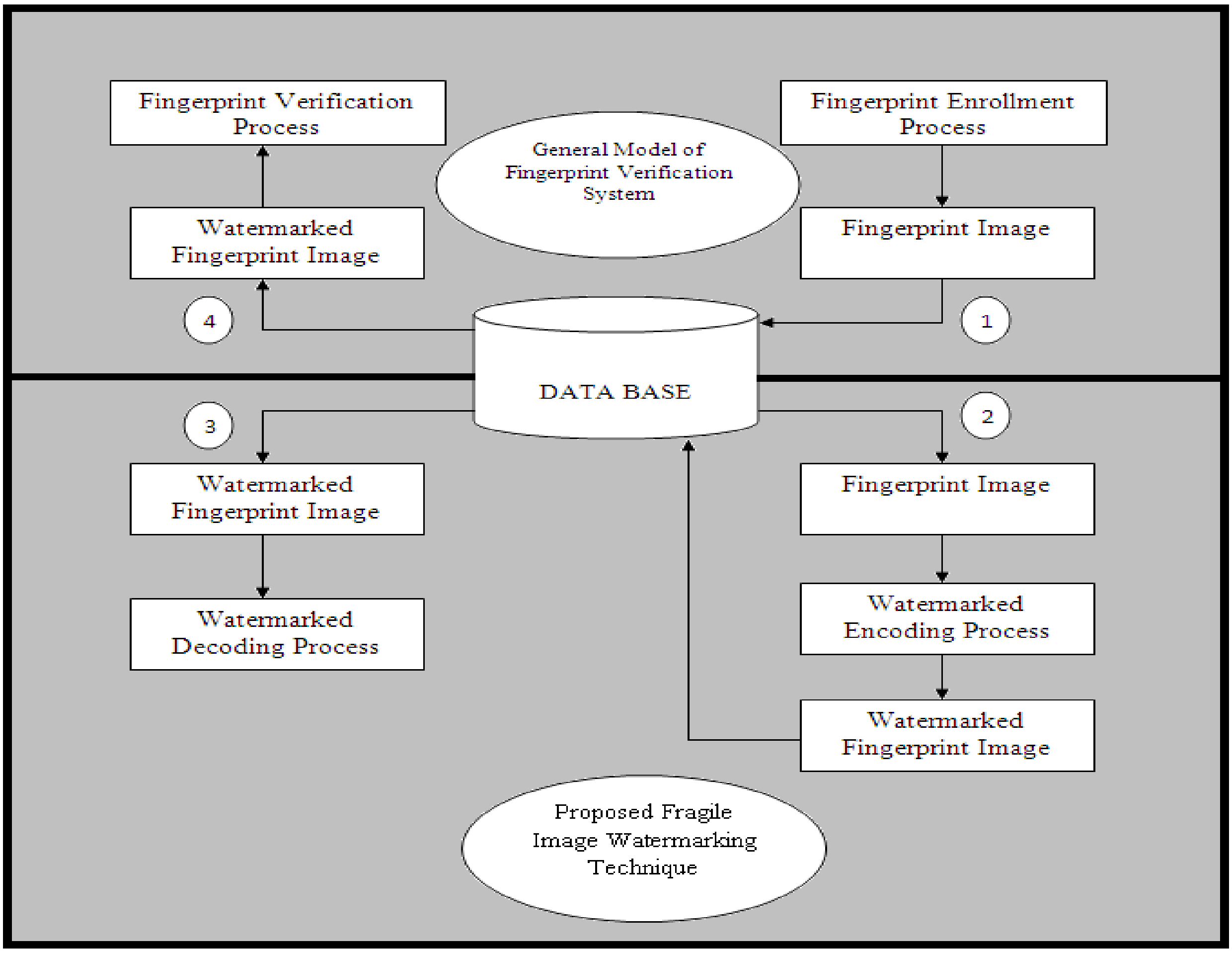
Fingerprint Verification Process
General Model of Fingerprint Verification System
Fingerprint Enrollment Process
Watermarked Fingerprint Image
Fingerprint Image
4
1
DATA BASE
3
2
Watermarked Fingerprint Image
Fingerprint Image
Watermarked Decoding Process
Watermarked Encoding Process
Watermarked Fingerprint Image
Proposed Fragile Image Watermarking Technique

**Figure: 4   Proposed Framework of Applying Information Hiding into Fingerprint Verification System**

## IV. EXPERIMENTAL RESULTS

There are two types of testing that have been done throughout the research process. The first test is the image quality testing. The second test is the watermarked fingerprint performance tested in the verification system. The first testing that has been done is the testing to evaluate the fingerprint image quality after the images were embedded with watermark data. This testing is needed to be done because the quality of the fingerprint images is crucial since the images will be used in the fingerprint verification system to compare the fingerprint minutiae for authentication process. 12 digits if ID number in text format is used as the

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

watermark data. Figure 5 shows the tested image and the ID number of the owner used. Figure 6 shows the watermarked image and the extracted correct ID number. This testing was able to embed 12 digits of ID number into the fingerprint image with capacity of around 14 to 16 kilobits of data. The embedding process will change the pixels value of the fingerprint data and because of this, an image quality testing has to be done to show the effects.

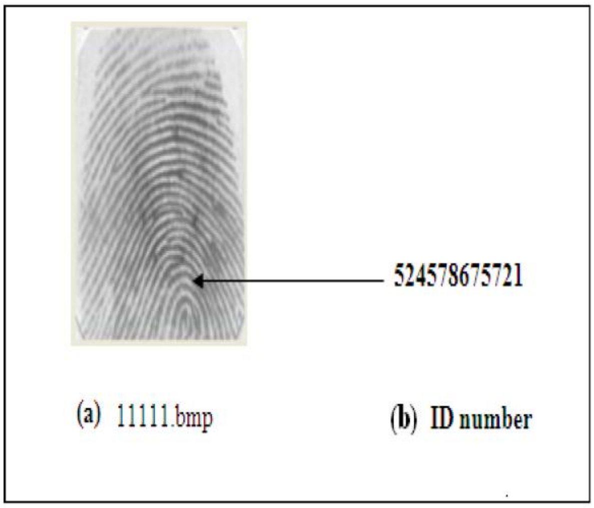

**Figure 5: Original fingerprint image and the Watermarked data**

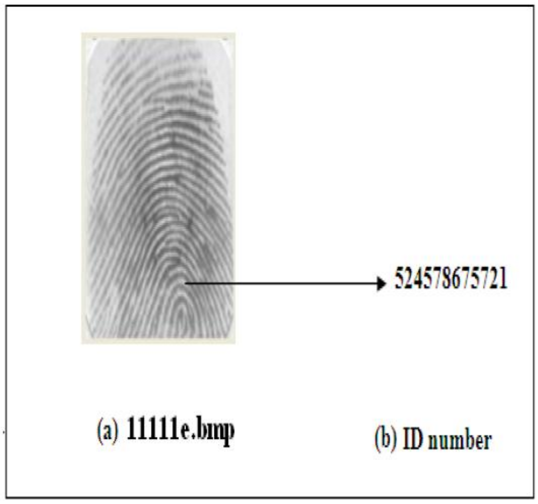

**Figure 6: Watermarked image and the extracted watermark data**

In conducting an image quality test, the mathematical software (MATLAB) has been used to compare the image quality between the original and the watermarked fingerprint templates by referring to the Mean Squared Error (MSE) and Peak to Signal Noise Ratio (PSNR) of both images. When computing MSE, the difference of the pixels is squared and the average is taken over the pixels in the image. This parameter is essentially capturing the changes that have been done to the image due to the watermark embedding process into the fingerprint template. The image that is perfectly produced from the original image will give the MSE reading of zero, while the image that is greatly differ from the original image will have the large MSE. The PSNR is closely related to MSE as can be seen in the equation below. The MSE reading is needed in order to produce the PSNR reading. PSNR is used to measure the invisibility of the embedded attributes (watermarked data) by referring to the perceptual degradation of the image quality. A PSNR is expressed in decibels (dB). PSNR is related to the mathematical equations of similarity between two images. The PSNR of an image will expectedly decreases as the modification of the pixels increase due to the watermark embedding. The PSNR metric that corresponds to be acceptable images for use in digital media has been estimated of range between 40dB to 50dB.

Their formulas are listed below:

$$\mathbf{PSNR = 10.log_{10} \frac{255^2}{MSE}\ (dB)}$$

$$\mathbf{MSE = \frac{1}{W.H} \sum_{i=1}^{W} \sum_{j=1}^{H} (\ F[i,j] - G[i,j]\ )^2}$$

Where F [i, j] and G [i, j] are the pixel values of the original and watermarked images at position (i, j) respectively; (W, H) and (w, h) specify the widths and the heights of the tested image and the watermarked data, respectively (C. K. Yang, 2004),

This formula has been translated into MATLAB coding as below:

$$D = F - G; \tag{1}$$

$$MSE = sum(D(:).*D(:))/prod(size(G)); \tag{2}$$

$$PSNR = 10*log10(255\wedge 2/mse); \tag{3}$$

D is the difference of pixel value between the original and watermarked images (F & G). The MSE and PSNR reading outputs will be presented in the table:

From table-I, we can see that all the PSNR values of the watermarked images are higher than 40dB with the average reading of 42.14 dB red channel, 42.50 dB for green channel and 41.81 dB for blue channel. This means that all the fingerprint images are still almost identical to the original one perceptually and only a small amount of pixels modification has been done to embed the watermark data. In conclusions, the embedded watermark data will not obviously change the pixel value of the fingerprint templates.

**TABLE – I: The MSE and PSNR of watermarked images compared to original images.**

| Images<br>(BMP Format) | Embedded<br>Data<br>(ID Number) | RGB<br>Plane | Mean Squared Error<br>(MSE) | Peak To Signal Noise<br>Ratio<br>(PSNR) |
|---|---|---|---|---|
| 11101 | 510989675612 | R | 2.1821 | 42.78 |
| | | G | 2.2135 | 42.99 |
| | | B | 1.8267 | 41.67 |
| 11111 | 524578675721 | R | 2.0091 | 41.72 |
| | | G | 2.3158 | 42.56 |
| | | B | 1.9813 | 41.28 |
| 11131 | 541216775125 | R | 1.8785 | 41.88 |
| | | G | 2.0813 | 42.30 |
| | | B | 1.8782 | 41.89 |
| 11161 | 561310457841 | R | 2.1680 | 42.67 |
| | | G | 2.3273 | 42.96 |
| | | B | 1.8982 | 41.87 |
| 11171 | 571115297124 | R | 2.0293 | 42.11 |
| | | G | 1.8117 | 41.87 |
| | | B | 2.1803 | 42.23 |
| 11191 | 639125697701 | R | 1.8819 | 41.98 |
| | | G | 2.0013 | 42.77 |
| | | B | 2.1372 | 42.99 |
| 11221 | 652475900142 | R | 1.9347 | 41.78 |
| | | G | 2.0972 | 42.13 |
| | | B | 1.9002 | 41.24 |
| 11271 | 680120013481 | R | 2.0991 | 42.47 |
| | | G | 2.1890 | 42.59 |
| | | B | 2.0113 | 42.11 |
| 11311 | 721475342101 | R | 1.9517 | 41.98 |
| | | G | 2.2649 | 42.87 |
| | | B | 2.2891 | 42.53 |
| 11351 | 741197724131 | R | 2.1548 | 42.57 |
| | | G | 2.1787 | 42.89 |
| | | B | 1.8781 | 41.57 |

The performance of watermarked fingerprint images also have been tested on biometric verification system (Verifinger 4.2 Evaluation).The image similarity reading and total process time for verification process are taken and been compared with the performance of the biometric identification system when using fingerprint images without watermarking data. Two tables (table-II and table-III) that show the results will be produced as the output of the testing that will show the difference of the performance in the fingerprint verification process

.

**TABLE-II: Fingerprint verification output process between original and watermarked images**

| Images<br>(BMP<br>Format) | Verification Process | Image Similarity | Total Process Time |
|---|---|---|---|
| 11101 | Successful | 1267 | 1s 417ms |
| 11111 | Successful | 1265 | 1s 571ms |
| 11131 | Successful | 1257 | 1s 271ms |
| 11161 | Successful | 1278 | 1s 330ms |
| 11171 | Successful | 1276 | 1s 356ms |
| 11191 | Successful | 1213 | 1s 352ms |
| 11221 | Successful | 1155 | 1s 387ms |
| 11271 | Successful | 1182 | 1s 403ms |
| 11311 | Successful | 1276 | 1s 327ms |
| 11351 | Successful | 1271 | 1s 401ms |

**Table-III: Fingerprint Verification output process between two original images**

| Images (BMP Format) | Verification Process | Image Similarity | Total Process Time |
|---|---|---|---|
| 11101 | Successful | 1267 | 1s 390ms |
| 11111 | Successful | 1268 | 1s257ms |
| 11131 | Successful | 1257 | 1s 327ms |
| 11161 | Successful | 1278 | 1s 302ms |
| 11171 | Successful | 1276 | 1s 368ms |
| 11191 | Successful | 1213 | 1s 336ms |
| 11221 | Successful | 1155 | 1s 256ms |
| 11271 | Successful | 1179 | 1s 299ms |
| 11311 | Successful | 1273 | 1s 213ms |
| 11351 | Successful | 1271 | 1s 307ms |

From table-II and table-III, we can see that the time taken for the identification process is not more than 2 seconds and this concludes that when the watermarked fingerprint images are used, it will not affect the standard time for verification process of the biometric identification system. The comparison of image similarity reading is also presented in figure 7. From the bar chart, we can see that the image similarity readings are the same on almost images. Only three fingerprint images (11111 .bmp , 11271 .bmp and 11311.bmp) shows a slightly differences of less than 4 units of similarity. These show that the similarity reading performance of the biometric identification system will not be affected when using the watermarked fingerprint images comparing to the fingerprint images that didn't use the watermarking method.

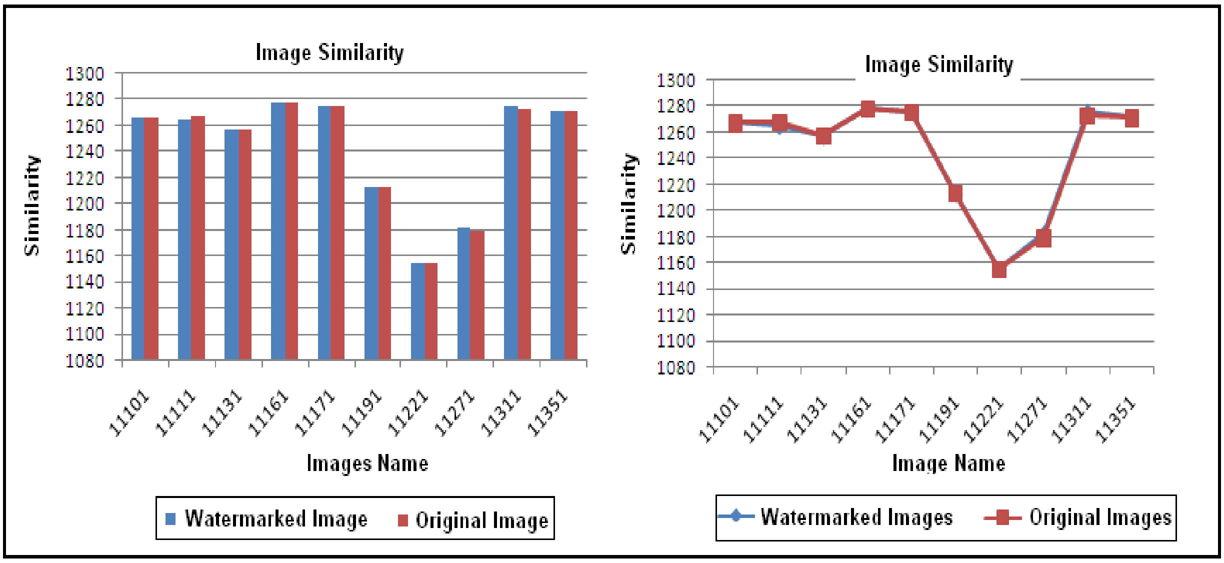

**Figure 7: Comparison of image similarity between original and watermarked fingerprint Images**

## V.CONCLUSION

A fragile image watermarking method for fingerprint images, in which we entered additional information into fingerprints, is described. The watermark data, which consist of the identification number, can be used in authenticating the host fingerprint image. The results show that the image quality if the fingerprint images are not being affected when proposed watermarking method is implemented. The performance on the recognition or retrieval accuracy of a personal identification system is also not affected when watermarked fingerprint images are used in the system. This proposed method hopefully can be used for image authentication to identify whether the image has been tampered by various image processing attacks such as noise addition and cropping.

## REFERENCES

1. S.Bruce, "*Inside risks: the uses and abuses of biometrics*," Communications of the ACM, Aug. 1999.
2. K. R. Geruta," Information Hiding on Wavelet Based Schemes under Consideration of Jpeg2000", University of Rostock, Department of Computer Science, Institute of Computer Graphics, Volume 42, Issue 8, 2000.
3. B. Pfitzmann, "Information Hiding Terminology," Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Versa, Berlin, 1996, pp. 347-356.
4. K. Rene Geruta,"Information Hiding on Wavelet Based Schemes under Consideration of Jpeg2000", University of Rostock, Department of Computer Science, Institute of Computer Graphics, 2001.
5. P.M. George, A.H. Albert, S.G. Laszlo, "Peak Signal to Noise Ratio Performance Comparison of JPEG and JPEG2OOO for Various Medical Image Modalities." Symposium on Computer Applications, 2000.

6. C. K Yang and C. S. Huang ,"A Novel Watermarking Techniques For Tampering Detection in Digital images," *Electronic Letters on Computer Vision and Image Analysis 3*, 2004 , pp. 1-12.
7. S. Bounkong, B.Toch, D.Saad and D. Lowe, "ICA for Watermarking Digital Images", *Journal of Machine Learning Research*, 2003, pp. 1471-1498.
8. A. K. Jain and U. Uludag, "Hiding biometric data*", IEEE Trans. Pattern Anal. Machine. Intelligence*, 25, No. 11, 2003. Pp. 1493-1498.
9. M.A. Suhail and M.S. Obaidat, "Digital Watermarking-based DCT and JPEG model*", IEEE Trans. On Instrumentation and Measurement*, vol. 52, No. 5, October 2003.
10. A.K.Jain, A. Ross, and U.Uludag, "*Biometrics Template security: Challenges and solutions*" in *Proc. of European Signal Processing Conference*, September 2005.
11. N. Johnson and S. Jajodia, "*:* Exploring Steganography Seeing the Unseen", *IEEE Computer*, 1998, pp. 26-34.
12. Elliott, S.J.; Massie, S.A.; Sutton, M.J. "*The Perception of Biometric Technology: A Survey*" Automatic Identification Advanced Technologies, 2007 IEEE Workshop on Volume, Issue, 7-8 June 2007 Page(s): 259 – 264.
13. N. K. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur,"Cancelable Biometrics: A Case Study in Fingerprints," in *Proceedings of the 18th International Conference on Pattern Recognition (ICPR 2006), 20-24 August 2006, Hong Kong, China. ICPR (4)*, 2006, pp. 370-373.
14. U. Uludag, B. Gunsel, and M Dalian "A spatial method for watermarking of fingerprint images" *Proc. First Inti. Workshop on Pattern Recognition in Information Systems*, Setubal, Portugal, 2001, pp. 26-33.
15. S. Asha, C. Chellappan, "Authentication of e-learners using multimodal biometric technology" in *IEEE- International Symposium on Biometric and Security Technologies, ISBAST 2008*," 23-24th , April 2008 . pp.1 – 6.
16. I.Hazwam," Fingerprint Template Security,"Masters thesis,University Utara Malaysia, 2007.
17. A. Arakala, J.Jeffers and K.J. Horadam,"Fuzzy Extractors for Minutiae-Based Fingerprint Authentication", in *International Conference on Biometrics*, 2007.
18. N.K.Ratha, J.H.Connell and R.M.Bolle,"An Analysis of Minutiae Matching Strength," *Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication*,2001, pp. 223-228.
19. U. Uludag and A.K. Jain, " Attacks on biometric systems: a case study in fingerprints", Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, pp. 622-633, San Jose, CA, January 18-22, 2004.