International Journal of Engineering Research and Development
e-ISSN : 2278-067X, p-ISSN : 2278-800X, www.ijerd.com
Volume 2, Issue 7 (August 2012), PP. 52-61

Hiding Additional Information in Fingerprint Images using Fragile Watermarking Technique

Jitendra Kumar Gothwal[1], Dr. Ram Singh[2]
[1]*Research Scholar, Department of Computer Sci. & Engg.,NIMS University,Jaipur,Rajasthan,India*
[2] *Professor, Department of Computer Sci. & Engg. , Jaipur, Rajasthan, India*

Abstract—One of the most emerging technologies for automatic people recognition is biometrics. The wide use of digital media in these recent days has led to an increase of digital piracy and tampering especially for biometric identification system. This work presents the concept of information hiding and one of its sub areas is called fragile image watermarking. While the biometrics techniques offer a reliable method for personal identification, the problem of security and integrity of the biometrics data is studied. This research work had proposed an architectural framework that will apply information hiding method into biometric identification system. A fingerprint watermarking method 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. The results show that the fingerprint images are not being affected when the watermarking method is implemented. 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, Information hiding, Fragile watermarking, Authentication system, Fingerprint

I. INTRODUCTION

Biometric methods for verifying, i.e. authenticating, someone's identity are increasingly being used. Today's commercially available biometric systems show good reliability. 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.

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].

Digital images had been widely used in various fields and areas in their applications such as medical, law enforcement, business and government agencies. Despite the obvious progress and various uses of digital multimedia, these developments carry with them a number of risks such as copyright violation, secret communication and data tampering.

The worries of threats and attacks that could be performed to the digital images could decrease the integrity and reliability of the digital data. Realizing the ease of editing and reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data such as digital images, digital audio and text document have become important concerns.

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.

Biometric-based Identification system, which use behavioural or physiological characteristics, are becoming increasingly popular compared to traditional knowledge-based or token-based system such as identification card, passwords, etc. 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 problern 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].

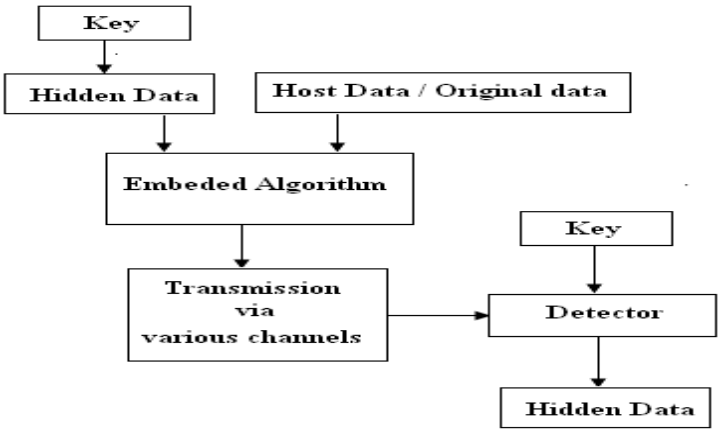

Fig. 1: Scenario of Information hiding

Biometrics systems are vulnerable to attacks, which can decrease their security. The attacks had been analysed and can be group into eight classes [11] [15]. One of them is attack on the template database (attack number 6 on Figure 2). 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.

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.

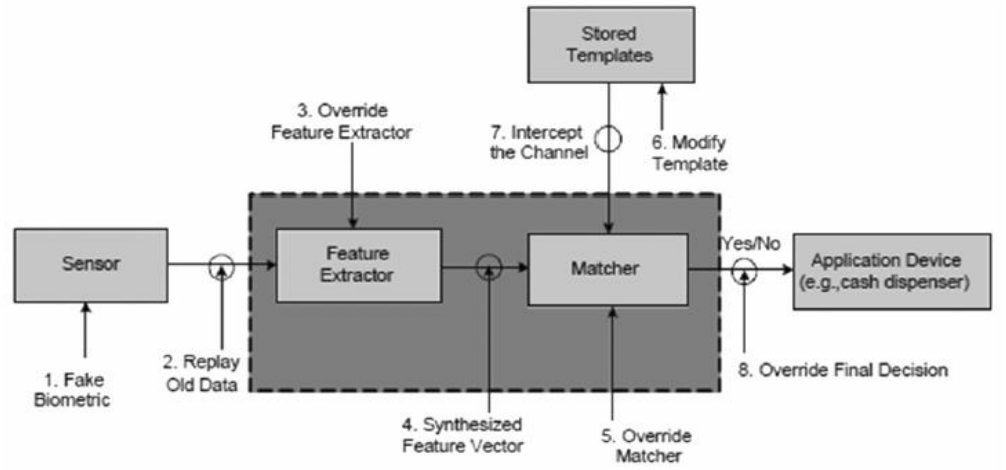

Fig. 2 Vulnerabilities in a Biometric System (Adapted from [8])

II. 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 (Figure 3). The typical system is proposed to be combined with an information hiding technique in order to enhance the security of the fingerprint images.

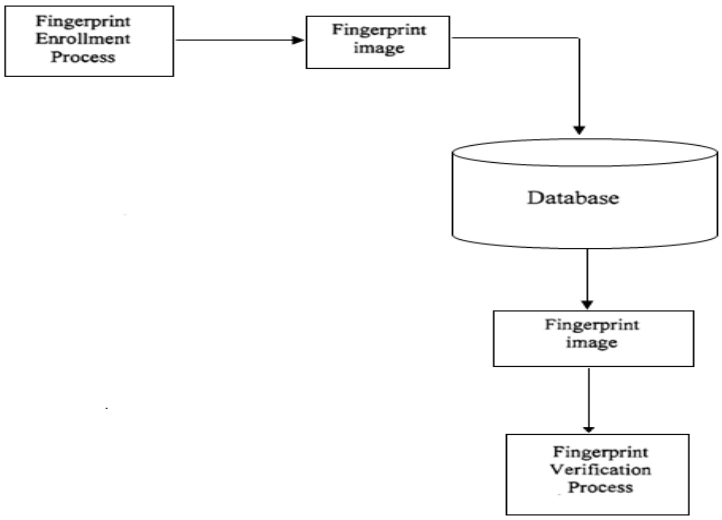

Fig. 3 General Model of Fingerprint Verification System

It can be seen in figure 3, the safety of the fingerprint image stored in the database can be are vulnerable to some attacks such as image tampering or image replacement. One of the main targets that attract the unwanted user to attack is the insecure fingerprint image templates stored in the database (Katha, K. N. et al., 2001; Uludag, U, and Anil, K J., 2004). In order to cater this problem, applying information hiding techniques into the system is necessary in order to authenticate the originality of the fingerprint image in the system database. One of the possible methods to enhance the security of the fingerprint template is by applying fragile image watermarking technique. This technique will work as a tamper proofing medium to detect whether the fingerprint template is genuine or it has been modified by unwanted user

As can be seen in Figure 4, 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 whole process of the proposed framework can be seen in Figure 4.

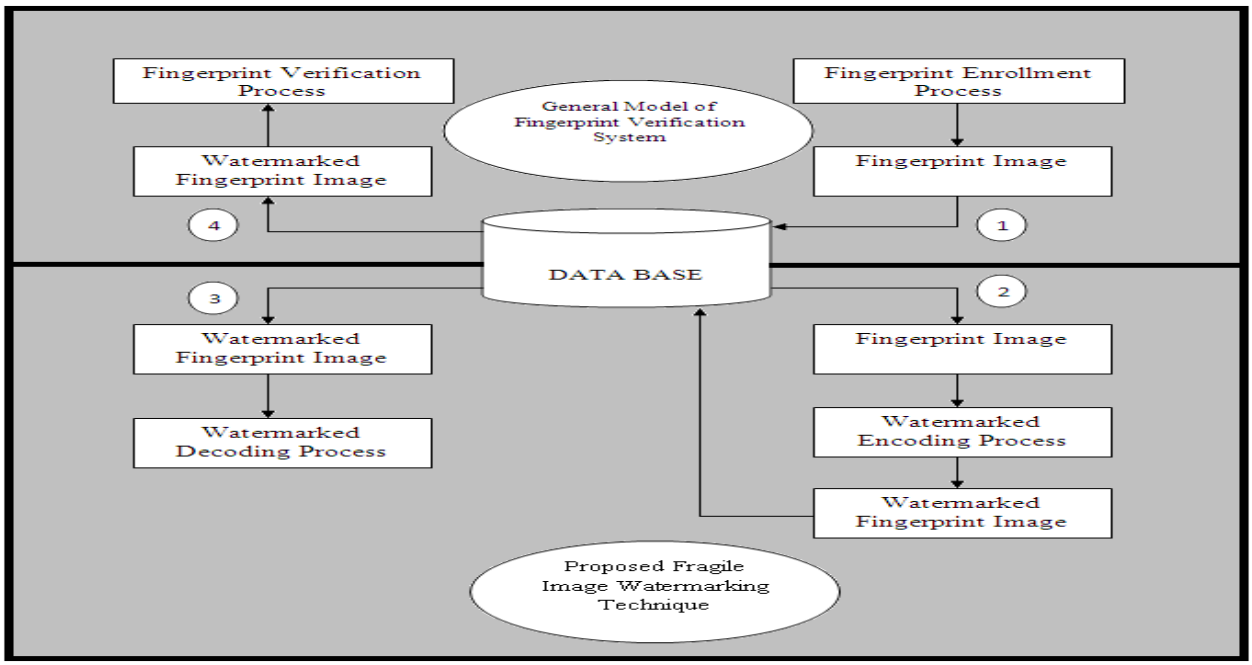

Fig. 4 Proposed Framework of Applying Information Hiding into Fingerprint Verification System

As shown in figure 4, this proposed architecture framework t 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 below part of figure 4, 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. This framework has been divided into four main phases which are fingerprint enrolment process, watermark encoding process, watermark decoding process and fingerprint verification process.The framework of embedding and detecting fragile image watermark is similar as the other watermarking system

FINGERPRINT ENROLLMENT PROCESS

The first phase of this framework is the fingerprint enrollment process. The enrollment process is shown in Figure 5 below.

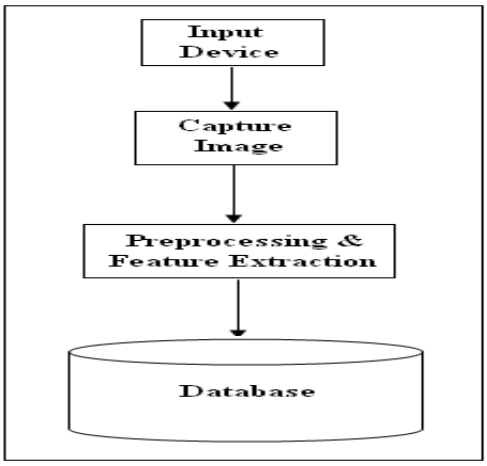

Fig. 5 Fingerprint Enrollment Process

First, the fingerprint image of an individual is captured by the input device sensor and for this case a fingerprint scanner had been used. The captured fingerprint will be the digital representation of the claimed individual. The data captured during the enrollment process may or may not be supervised by the human depending on the application. The further process will be the feature extraction process where a compact, but expressive representation template will be generated. The template then will be stored into the database of the system and this database may be updated over time

WATERMARK ENCODING & DECODING PROCESS

For the second phase, the fingerprint image template is embedded with the additional information (watermark) to protect the template from being tampered. In order to do this, a fragile image watermarking technique has been used. Figure 6 below shows the process of embedding the watermark data.

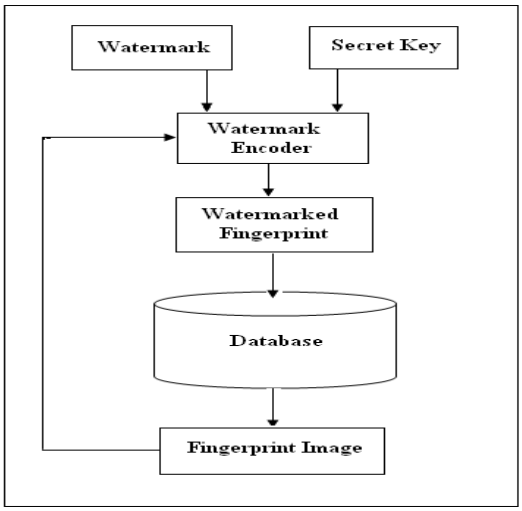

Fig. 6 The Watermark Encoding Process

First, the fingerprint template is taken out from the database where it will be embedded with a watermark data. Before the embedding process, the watermark data is converted into a bit stream. Then a random number generator is initialized with a secret key that will generate the pixel locations in the host image (fingerprint template) to watermark the additional information. The additional information will be hidden in the fingerprint template and it will be imperceptible to human visual system. After the embedding process, the watermarked fingerprint template will be stored back into the database.

The watermark decoding process will be occurred in the third phase. This phase is done just before the fingerprint matching process to authenticate the stored fingerprint template first before it will be used. This process will enhance the security of the fingerprint verification system. Figure 7 shows the watermark decoding process.

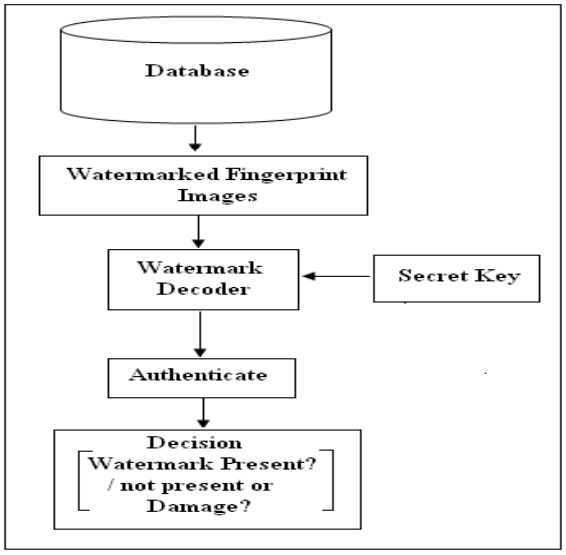

Fig. 7 Watermark Decoding Process

The watermark decoding process will extract the watermark that is hidden in the fingerprint template. The secret key is used to identify the pixel locations in the fingerprint template that has been used to embed the watermark data. The presence of the watermark data will authenticate the genuineness of the fingerprint template. If the watermark data cannot be extracted, this means that the fingerprint template may be tampered or added into the database by the unauthorized individual. The recovered watermark data also can be used as the second source of authenticity either automatically or by human in a supervised biometric application.

FINGERPRINT VERIFICATION PROCESS

The fourth phase of this framework will be the fingerprint verification process (Figure 8).

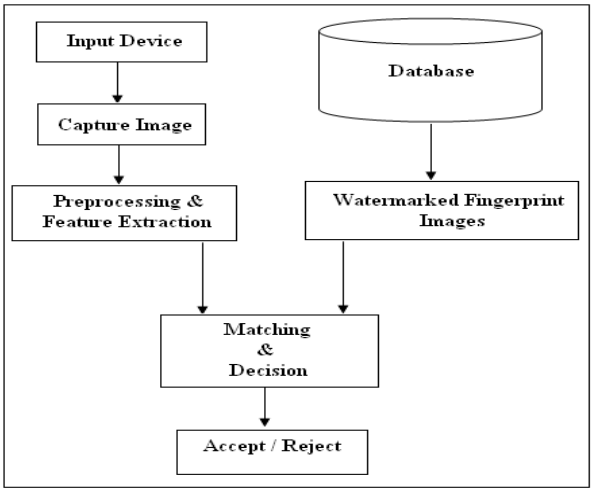

Fig. 8 The Fingerprint Verification Process

In this phase, the input device (fingerprint sensor) will capture the features of the fingerprint image whether directly from the finger of the user or from the smart card and it is compared with the stored watermarked fingerprint template to generate matching scores. The number of matching fingerprint minutiae between the input feature and the fingerprint template image is determined and the matching score is reported either to accept or reject the individual.

III. 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 last testing is watermark embedding capacity limit.

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 watermark data. Figure 9 shows the tested image and the ID number of the owner used. Figure 10 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.

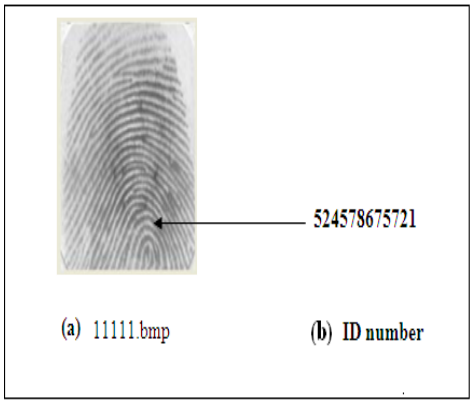

Fig. 9 Original fingerprint image and the watermarked data

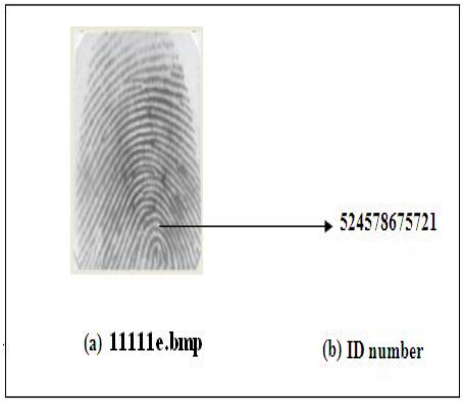

Fig.10 Watermarked image and the extracted watermark data

In conducting an image quality test, the mathematical software (MATLAB r2OO6a) 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.

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 (P. M. George, A. H. Albert, S. G. Laszlo, 2003).

Their formulas are listed below:

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

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

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;                                  (1)

MSE = sum(D(:).*D(:))/prod(size(G));        (2)

PSNR = 10*log10(255^2/mse);                 (3)
```

D is the difference of pixel value between the original and watermarked images (F & G). The reading outputs of the process were taken and will be presented in the results and analysis topic. The MSE and PSNR reading outputs will be presented in the table form.

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 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.The results of the fingerprint image quality testing were presented as shown in Table-I. The result is the output of the Peak to Signal Noise Ratio calculation done by using Matlab software.

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

Images (BMP Format)	**Embedded Data (ID Number)**	**RGB Plane**	**Mean Squared Error (MSE)**	**Peak To Signal Noise Ratio (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
11121	531672883447	R	2.0127	41.77
		G	2.2753	42.46
		B	1.8362	41.63
11131	541216775125	R	1.8785	41.88
		G	2.0813	42.30
		B	1.8782	41.89
11141	554321754989	R	2.1229	42.43
		G	2.2991	42.57
		B	1.9811	41.68
11151	557123812711	R	2.0273	42.18
		G	2.3453	42.79
		B	1.8792	41.87
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
11181	585612881297	R	1.9519	41.68
		G	2.1898	42.49
		B	1.9692	41.87
11191	639125697701	R	1.8819	41.98
		G	2.0013	42.77
		B	2.1372	42.99
11211	641177687012	R	1.9112	41.63
		G	1.9533	41.78
		B	1.9112	41.63
11221	652475900142	R	1.9347	41.78
		G	2.0972	42.13
		B	1.9002	41.24
11231	656775513751	R	1.8978	41.67
		G	2.2659	42.89
		B	1.9513	41.91
11241	658114329811	R	2.0578	42.43
		G	2.0596	42.51
		B	1.9761	41.97
11251	661432768842	R	1.8911	41.88
		G	2.3547	42.59
		B	1.8109	41.67
11261	674457713265	R	2.2660	42.54
		G	2.2817	42.77
		B	1.8956	41.76
11271	680120013481	R	2.0991	42.47
		G	2.1890	42.59
		B	2.0113	42.11
11281	691375524092	R	1.9112	41.89
		G	2.1901	42.36

		B	2.0723	42.17
11291	718792464317	R	1.8448	41.37
		G	2.3892	42.79
		B	1.9112	41.77
11301	719245687144	R	2.2576	42.41
		G	2.0803	42.13
		B	1.8796	41.62
11311	721475342101	R	1.9517	41.98
		G	2.2649	42.87
		B	2.2891	42.53
11321	722577478904	R	2.0923	42.78
		G	2.2179	42.89
		B	1.7986	41.52
11331	725517650988	R	2.2441	42.41
		G	1.9764	41.86
		B	1.8988	41.35
11341	731427568814	R	2.0917	42.57
		G	1.9118	41.72
		B	1.9002	41.51
11351	741197724131	R	2.1548	42.57
		G	2.1787	42.89
		B	1.8781	41.57

Table-I shows all the fingerprint templates that have been used for the testing. An ID number consist of 12 digits has been embedded in the fingerprint images and will be used as the watermark data. By using the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) equation, the MSE and PSNR results of each of the images have been produced.

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.

The results of the performance testing were presented in table-II and III shown below. These performance results were taken by the Verification output and the result of the process were done by the Verifmger 4.2 software.

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

Images (BMP Format)	**Verification Process**	**Image Similarity**	**Total Process Time**
11101	Successful	1267	1s 417ms
11111	Successful	1265	1s 571ms
11121	Successful	1266	1s 405ms
11131	Successful	1257	1s 271ms
11141	Successful	1272	1s 403ms
11151	Successful	1278	1s 329ms
11161	Successful	1278	1s 330ms
11171	Successful	1276	1s 356ms
11181	Successful	1223	1s 317ms
11191	Successful	1213	1s 352ms
11211	Successful	1213	1s 399ms
11221	Successful	1155	1s 387ms
11231	Successful	927	1s 393ms
11241	Successful	1278	1s 399ms
11251	Successful	1276	1s 405ms
11261	Successful	1262	1s 417ms
11271	Successful	1182	1s 403ms
11281	Successful	1274	1s 356ms
11291	Successful	1278	1s 355ms
11301	Successful	1271	1s 423ms
11311	Successful	1276	1s 327ms
11321	Successful	1277	1s 399ms
11331	Successful	1277	1s 399ms

11341	Successful	1276	1s 397ms
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
11121	Successful	1262	1s 307ms
11131	Successful	1257	1s 327ms
11141	Successful	1272	1s 383ms
11151	Successful	1278	1s 345ms
11161	Successful	1278	1s 302ms
11171	Successful	1276	1s 368ms
11181	Successful	1223	1s 227ms
11191	Successful	1213	1s 336ms
11211	Successful	1213	1s 323ms
11221	Successful	1155	1s 256ms
11231	Successful	927	1s 271ms
11241	Successful	1278	1s 306ms
11251	Successful	1276	1s 317ms
11261	Successful	1262	1s 302ms
11271	Successful	1179	1s 299ms
11281	Successful	1274	1s 278ms
11291	Successful	1278	1s 321ms
11301	Successful	1271	1s 298ms
11311	Successful	1273	1s 213ms
11321	Successful	1277	1s 217ms
11331	Successful	1277	1s 253ms
11341	Successful	1276	1s 279ms
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 11. From the bar chart, we can see that the image similarity readings are the same on almost images. Only three fingerprint images (11111 .bmp, 11121 .bmp and 11271 .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.

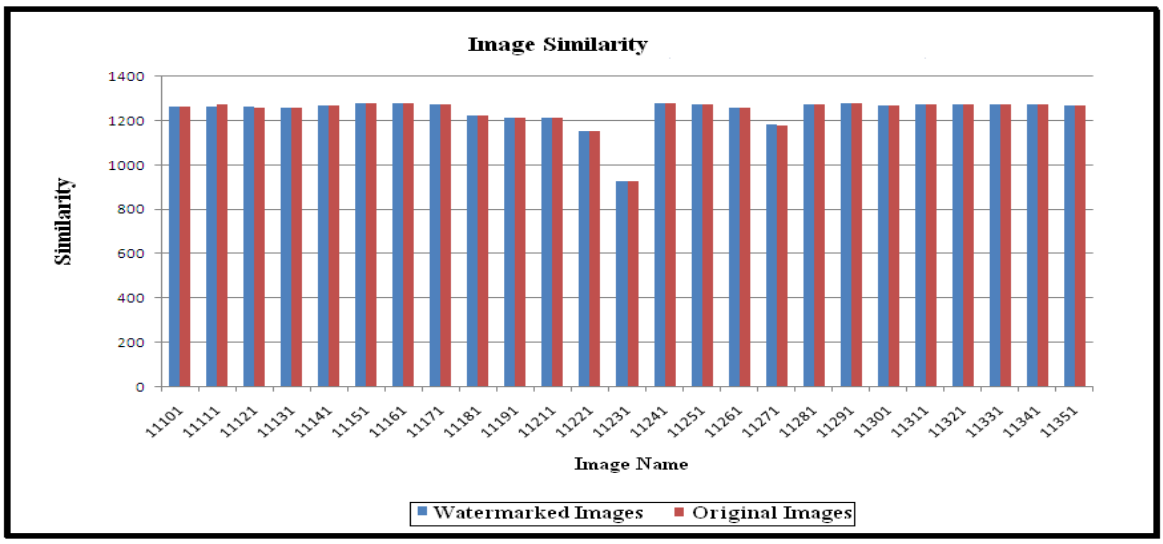

Fig. 11 Comparison of image similarity between original and watermarked fingerprint Images

IV. 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]. 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.

[2]. Geruta, K. Rene.,"*Information Hiding on Wavelet Based Schemes under Consideration of Jpeg2000*", University of Rostock, Department of Computer Science, Institute of Computer Graphics, 2001.

[3]. George P. M , Albert A. H. , Laszlo S. G. (2003). "*Peak Signal to Noise Ratio Performance Comparison of JPEG and JPEG2OOO for Various Medical Image Modalities*." *Symposium on Computer Applications.*

[4]. Katha K. N., Jonathan H. C., & Ruud M. B. (2001). *An Analysis of Minutiae Matching Strength*. Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228.

[5]. C. K Yang, C. S. Huang (2004) "*A Novel Watermarking Techniques For Tampering Detection in Digital images*" Electronic Letters on Computer Vision and Image Analysis 3, (pp. I-'12).

[6]. Uludag U., & Anil K. J. (2004). *Attacks on Biometrics System: A Case Study in Fingerprints. Proc. SPIE-El 2004, Security, Steganography and Watermarking of Multimedia contents* VI, pp. 622-633.

[7]. Bounkong, S., Toch, B., Saad, D. and Lowe, D. (2003) "*ICA for Watermarking Digital Images*", Journal of Machine Learning Research, Pp. 1471-1498.

[8]. A. K. Jain and U. Uludag, "*Hiding biometric data", EEE Trans. Pattern Anal. Machine. Intelligence*, **25**, No. 11, pp. 1493-1498, 2003.

[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]. Jain A.K, Ross Arun and Uludag.U. "*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]. M. Yeung and S. Pankanti, "*Verification watermarks on fingerprint recognition and retrieval*," in Proc. SPIE, Security and Watermarking of Multimedia Contents, vol. 3657, pp. 66–78, (San Jose, USA), January 1999.

[13]. 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.

[14]. N. K. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur: *Cancelable Biometrics: A Case Study in Fingerprints*. Proceedings of the 18th International Conference on Pattern Recognition (ICPR 2006), 20-24 August 2006, Hong Kong, China. ICPR (4) 2006: 370-373

[15]. U. Uludag, B. Gunsel, and M Dalian "*Aspatial method for watermarking of fingerprint images*" Proc. First Inti. Workshop on Pattern Recognition in Information Systems, Setubal, Portugal, 2001, pp. 26-33.