# Biometric Template Security Using Invisible Watermarking With Minimum Degradation in Quality of Template

Rajkumar Yadav*
Assistant Professor
U.I.E.T, M.D.U, Rohtak
rajyadav76@rediffmail.com

Kamaldeep
Assistant Professor
*Savera Group of Institutions (Gurgaon)*
*kamalmintwal@gmail.com*

Ravi Saini
Project Fellow
U.I.E.T, M.D.U, Rohtak
*ravisaini1988@rediffmail.com*

Rainu Nandal,
U.I.E.T, M.D.U, Rohtak

***Abstract*— In this paper, we present an approach to enhance the Biometric Template Security by using Invisible Watermarking. For embedding the watermark in the Biometric Template, we used Parity Checker Method [2]. The use of Parity Checker Method ensures that the change in Biometric Template should be minimum. The watermark that is embedded in the Biometric Template may contain person's name, person's address or some unique features of the person. The same watermark is embedded four times in the Biometric Template to enhance its security so that if one watermark is changed by attacker, the other watermark remains intact. For each biometric template there will be a secret key that is used for embedding of watermark. The maintenance of secret key will be responsibility of database manager. The same key can be used for all biometric templates which reduces the responsibility of database manager up to a greater extent but at the cost of security. So, we used the separate key for each Biometric Template.**

***Keywords- Biometrics, Watermarking, Steganography, Security, Parity Checker.***

## I. Introduction

Biometric 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 or her unique physical characteristics [3]. Basic modules of a biometric system are:

- Enrollment Unit

The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

- Feature Extraction Unit

This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

- Matching Unit

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score of match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one to many matching).

- Decision Maker

This module accepts or rejects the user based on a security threshold and matching score.

Biometrics offers greater security and convenience than traditional identify authentication systems (based on passwords and cryptographic keys) since biometric 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 in a vital security issue in biometrics [4]. Biometric Template can be protected by using watermarking. Watermarking is the process of embedding information such as Owner Name, Company Logo etc. in the host data [5]. General image watermarking methods can be divided into two groups according to the domain of application of watermarking. In spatial domain methods [6], the pixel values in the image channel(s) are changed. In spectral-transform domain methods, a watermark signal is added to the host image in a transform domain such as the full-frame DCT domain [7]. It is application of steganography.

In this paper, we attempt to secure the biometric template by using the Spatial Domain Techniques of Watermarking. We have masked the watermarked information in such a way that changes in biometric template after embedding of watermark would be minimum. For this purpose, we used the Steganography Method known as Parity Checker Method [2]. We embed the watermark four times for further security enhancement of biometric template so that if attacker forges the one watermark then other watermarks will remain intact.

The rest of the paper is organized as follows:

In section 2, various types of attacks on Biometric Systems are discussed. Section 3 gives our proposed system. Section 4 includes results and analysis of the proposed approach. In section 5, some emphasis is given on conclusion and future work.

## II. ATTACKS ON THE BIOMETRIC SYSTEM [8]

### *A. First attack*

Attack on the sensor. Sensor can be overridden by presenting fake Biometrics [U.K.Biometrics Workshop Group]. Like a fake finger, face mask or a copy of signature.

### *B. Second attack*

The Attack on the channel between the sensor and the feature extractor. Biometrics which was submitted can be resubmitted or replayed by bypassing the sensor. Like an old copy of fingerprint or face image. Prepare Your Paper Before Styling

### *C. Third attack*

Define Attack on the feature extractor. Feature extractor can be override by attacking it and forcing it to produce feature values selected by the hacker.

### *D. Fourth attack*

Attack on the channel between the feature extractor and the matcher. Features extracted by the extractor can be replaced by a different feature set. This type of attack is difficult because the feature extractor and matcher are not separate. This attack is possible only if the matcher is remote and the features extracted have to be sent to the matcher for matching purpose.

### *E. Fifth attack*

Attack on the matcher. Matcher can be overridden by attacking it and forcing it to produce high or low matching score irrespective of the input.

### *F. Sixth attack*

Attack on the stored database. The database can be local or remote. Templates which are stored at the time of enrollment can be attacked by modifying one or more templates in the database. This could result in fraudulent authorization of an individual or a denial of service.

### G. Seventh attack

Attack Attack on the channel between the system's database and the matcher. Respective template is selected and sent through a channel to the matcher for identification. This template can be changed accordingly by the hacker.

### H. Eighth attack

Attack on the channel between the matcher and application device. The decision whether the user can access the application device can be changed by the hacker accordingly [10].

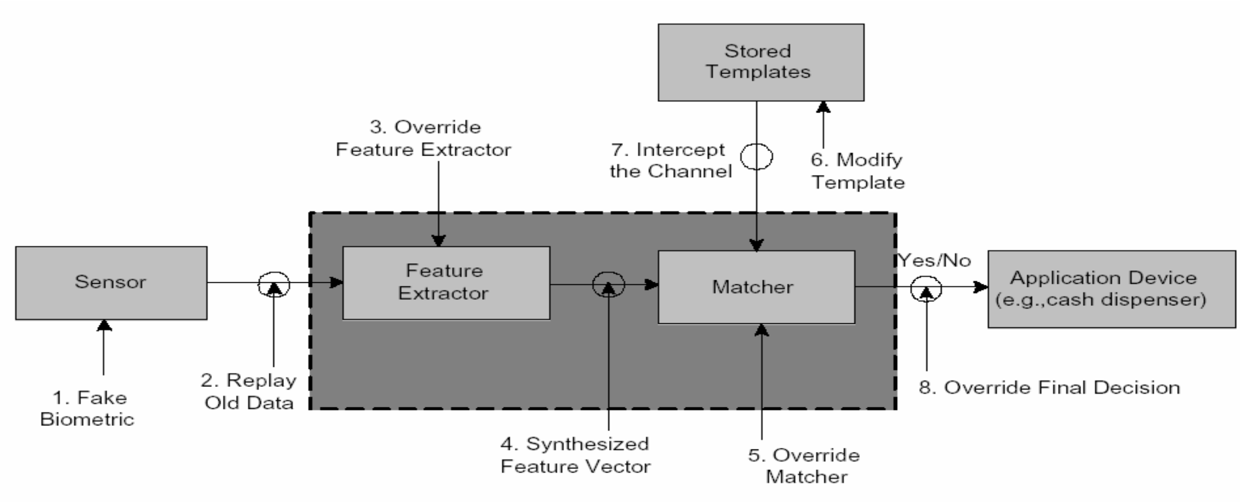


Figure 1. Attacks on the Biometric System

## III. THE PURPOSED SYSTEM

In our system, we used the watermarking for security of biometric template. Biometric template can be replaced or forged by attacker. But, in our system, if attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden. If attacker changes the secure biometric template (i.e. Biometric template with watermark information) with forge biometric template then it gives the clue to database manager that something has gone wrong with biometric template because in forge biometric template either the watermark will not be present or will be present at wrong pixel positions. For the insertion of watermark information in biometric template we used the Parity Checker Method [2]. Also, we inserted the watermark information four times in biometric template so that if attacker is able to change watermark at one place, the watermark at other places remain intact. The process of securing the biometric template is shown in Figure 2.

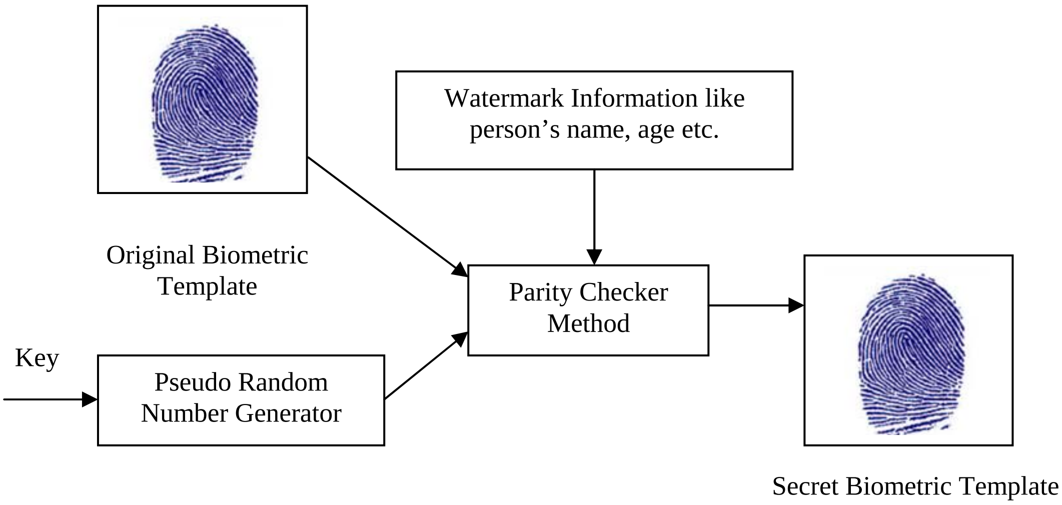

Watermark Information like person's name, age etc.
Original Biometric Template
Parity Checker Method
Key
Pseudo Random Number Generator
Secret Biometric Template

Figure 2. Creation of Secret Biometric Template

### *A. Algorithm*

Step 1: Read the watermark information that we want to hide in the biometric template.

Step 2: Read the biometric template

Step 3: Find out the pseudorandom pixel location in the biometric template where watermark is to be inserted by using pseudorandom number generator which is seeded with the secret key.

Step 4: If at a pixel location we want to hide 0, then go to step 5 else go to step 6.

Step 5: a) Check whether there exists odd parity at the selected pixel location, then insert 0 at the pixel location (no change in pixel value is required in this case). Go to END.
b) If even parity exists, then make the odd parity at that location by adding or subtracting 1 to that pixel location (change in pixel is required in this case). Go to END.

Step 6: a) Check whether there exists even parity at the selected pixel location, then insert 1 at the pixel location (no change in pixel value is required in this case). Go to END.
b) If odd parity exists, then make the even parity at that location by adding or subtracting 0 to that pixel location (change in pixel is required in this case). Go to END.

Step 7: END.

### *B. Key Managament*

A separate key is required for each biometric template for watermarking. This key is used by pseudo-random number generator for generation of pixel locations in biometric template where watermark is to be inserted. This key must be kept secret so that attacker cannot forge the biometric template. The key management is the responsibility of database manager. The Key management process is shown by Figure 3.

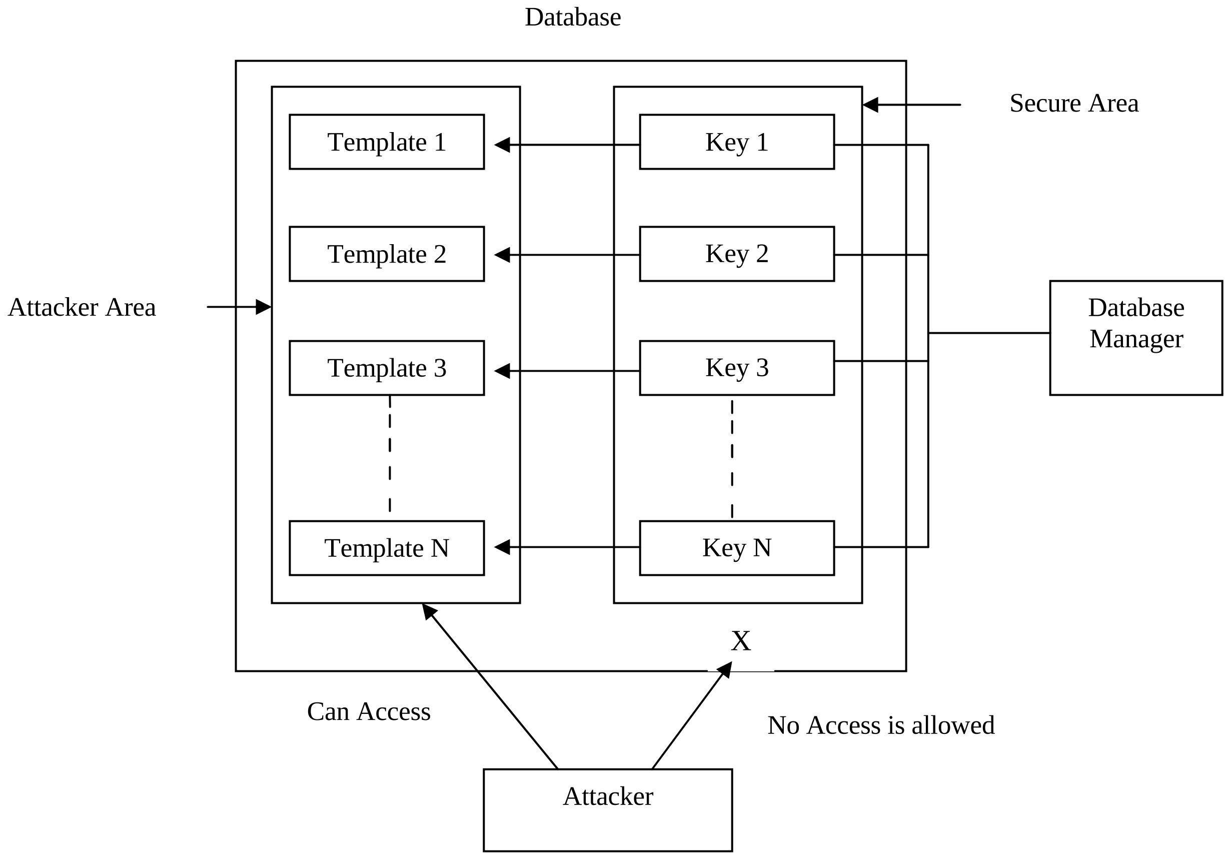
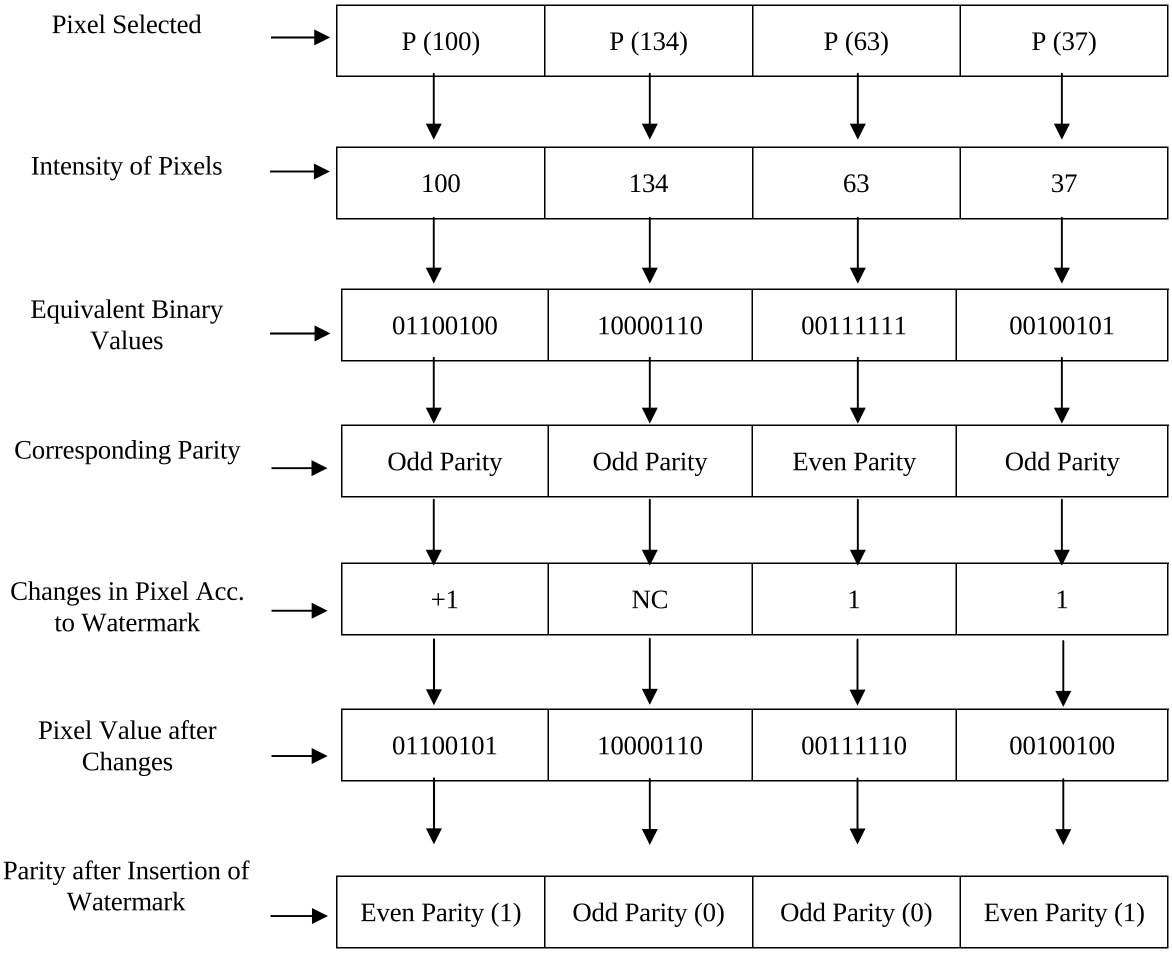


Figure 3. Key Management

### C. Practical Example

Suppose the watermark is 1001 and selected pixels of biometric template by pseudo-random number generator are P (100), P (134), P (63), P (37) where P(i) means Pixel P has intensity i. The insertion of watermark 1001 is shown by Figure 4.



| | | | | |
|---|---|---|---|---|
| Pixel Selected | P (100) | P (134) | P (63) | P (37) |
| Intensity of Pixels | 100 | 134 | 63 | 37 |
| Equivalent Binary Values | 01100100 | 10000110 | 00111111 | 00100101 |
| Corresponding Parity | Odd Parity | Odd Parity | Even Parity | Odd Parity |
| Changes in Pixel Acc. to Watermark | +1 | NC | 1 | 1 |
| Pixel Value after Changes | 01100101 | 10000110 | 00111110 | 00100100 |
| Parity after Insertion of Watermark | Even Parity (1) | Odd Parity (0) | Odd Parity (0) | Even Parity (1) |

Figure 4. Insertion of watermark

## IV. Results and analysis

### A. Analysis based upon Matching Score

We hide the watermark in the biometric template and then try to check whether the matching score between enrolled template and secret template cross the Threshold Value or not. We also check Matching Scores between original template (without watermark) and enrolled template. By comparing the Matching Scores of original template and enrolled template with the Matching Score of secret template and enrolled template we found favorable results. We divide the result into four levels based upon the number of times the watermark is inserted in the biometric template. Figure 5 shows the original template. Figure 6, 7, 8 & 9 shows the secret template with watermark (Kamaldeep) inserted one time, two times, three times and four times respectively. Table I, Table II, Table III & Table IV shows the comparison of matching scores of five different enrolled templates with the original template and secret template. When watermark is inserted one time, two times, three times and four times respectively.

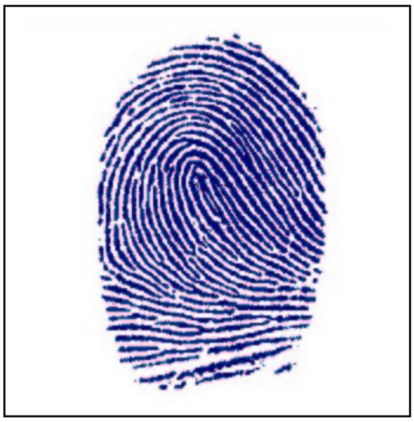


Figure 5. Original Template

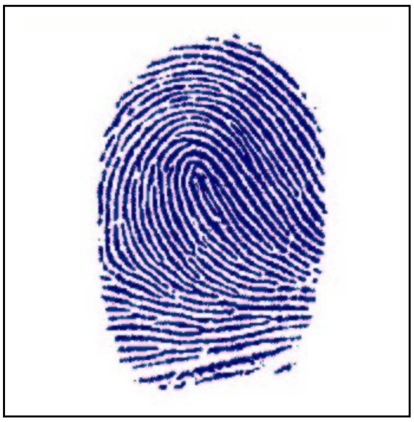


Figure 6. Secret template with watermark ‘kamaldeep’ inserted one time.

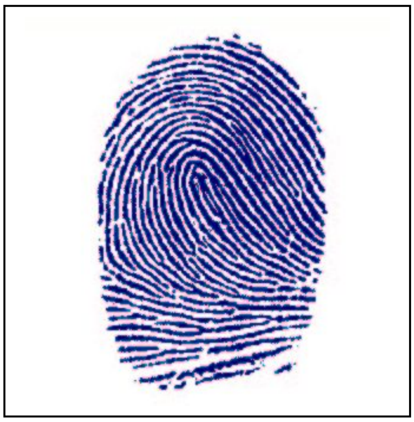


Figure 7. Secret template with watermark ‘kamaldeep’ inserted two time.

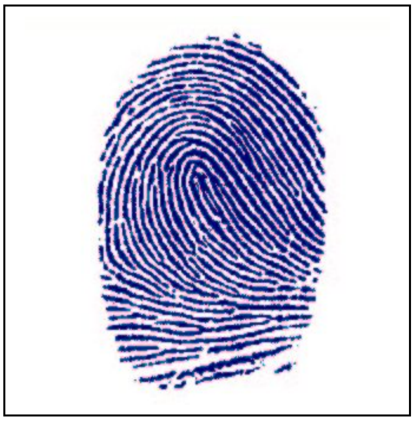


Figure 8. Secret template with watermark ‘kamaldeep’ inserted three time.

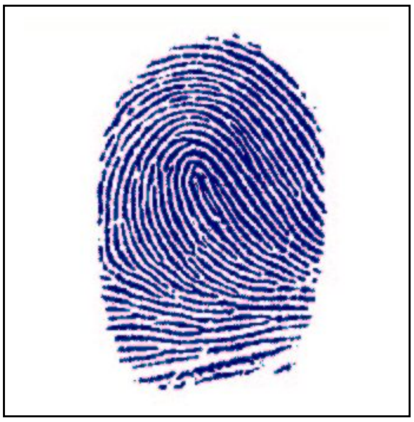


Figure 9. Secret template with watermark ‘kamaldeep’ inserted four times.

TABLE I. COMPARISON WHEN WATERMARK IS INSERTED ONE TIME

| **Enrolled Template** | **Threshold Value** | **Matching Score between original template & enrolled template** | **Matching Score between secret template & enrolled template** |
|---|---|---|---|
| ***Template – I*** | 70 | 79 | 76 |
| ***Template – II*** | 70 | 85 | 84 |
| ***Template – III*** | 70 | 92 | 90 |
| ***Template – IV*** | 70 | 83 | 77 |
| ***Template – V*** | 70 | 77 | 75 |

TABLE II. COMPARISON WHEN WATERMARK IS INSERTED TWO TIME

| Enrolled Template | Threshold Value | Matching Score between original template & enrolled template | Matching Score between secret template & enrolled template |
|---|---|---|---|
| ***Template – I*** | 70 | 79 | 76 |
| ***Template – II*** | 70 | 85 | 84 |
| ***Template – III*** | 70 | 92 | 90 |
| ***Template – IV*** | 70 | 83 | 77 |
| ***Template – V*** | 70 | 77 | 75 |

TABLE III. COMPARISON WHEN WATERMARK IS INSERTED THREE TIME

| Enrolled Template | Threshold Value | Matching Score between original template & enrolled template | Matching Score between secret template & enrolled template |
|---|---|---|---|
| ***Template – I*** | 70 | 79 | 72 |
| ***Template – II*** | 70 | 85 | 79 |
| ***Template – III*** | 70 | 92 | 82 |
| ***Template – IV*** | 70 | 83 | 75 |
| ***Template – V*** | 70 | 77 | 73 |

TABLE IV. COMPARISON WHEN WATERMARK IS INSERTED FOUR TIME

| Enrolled Template | Threshold Value | Matching Score between original template & enrolled template | Matching Score between secret template & enrolled template |
|---|---|---|---|
| ***Template – I*** | 70 | 79 | 71 |
| ***Template – II*** | 70 | 85 | 75 |
| ***Template – III*** | 70 | 92 | 79 |
| ***Template – IV*** | 70 | 83 | 74 |
| ***Template – V*** | 70 | 77 | 72 |

The comparison that is shown in Table I, Table II, Table III and Table IV are also shown by Figure 10, Fig 11, Fig 12 & Fig 13 respectively. From Fig 10,Fig11, Fig12 and Fig13, we can conclude that the matching score between secret template and enrolled template remains always greater than the threshold value which shows that we will get correct result of biometric system after the insertion of watermark information. Also, the matching score between secret template and enrolled template remains close with matching score of original template and enrolled template. As we increase the size of watermark information embedded in the biometric template the matching score will degrade and may come below the threshold value. So, we try to keep the size of watermark information as less as much possible.

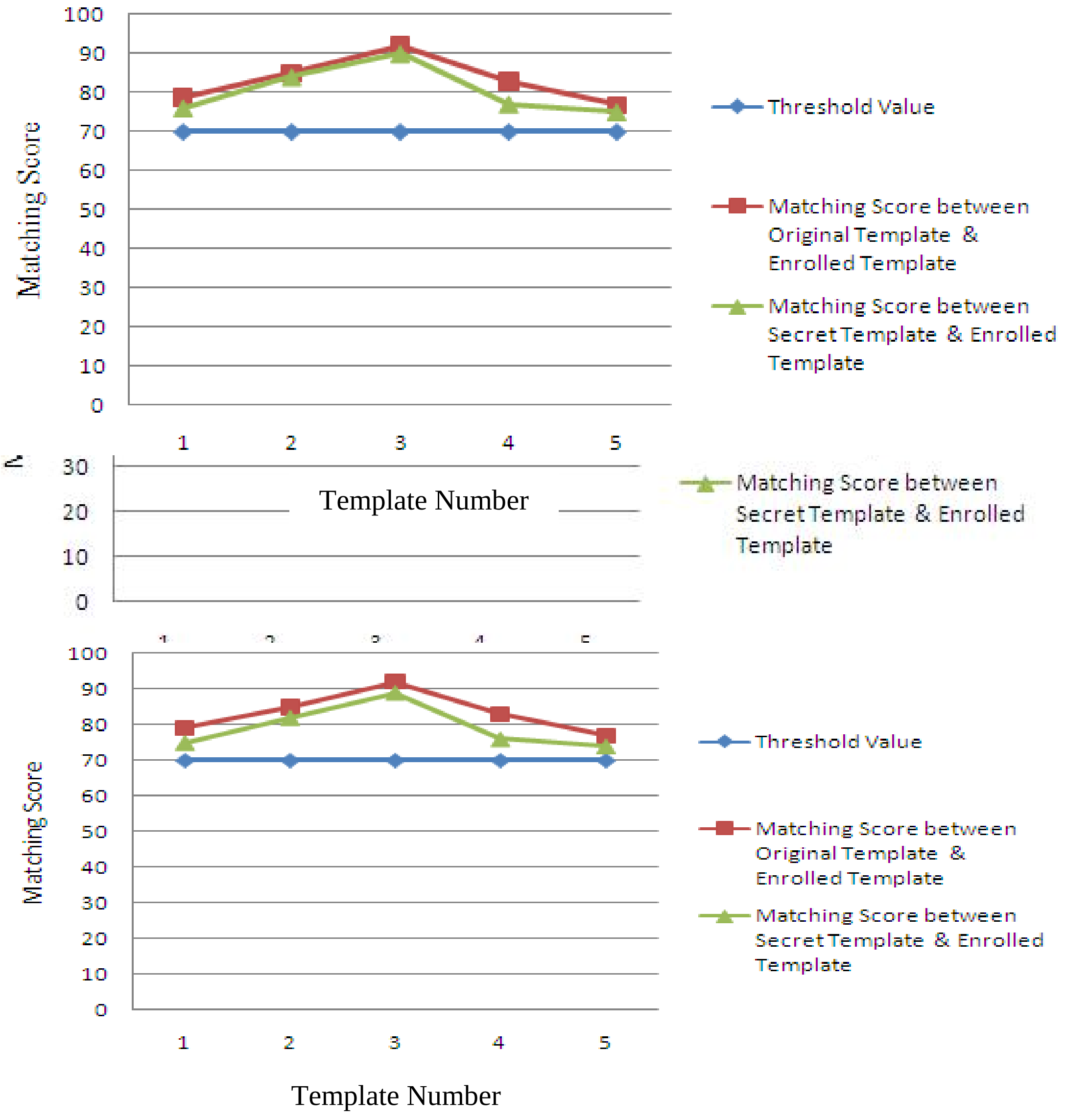


Figure 11.

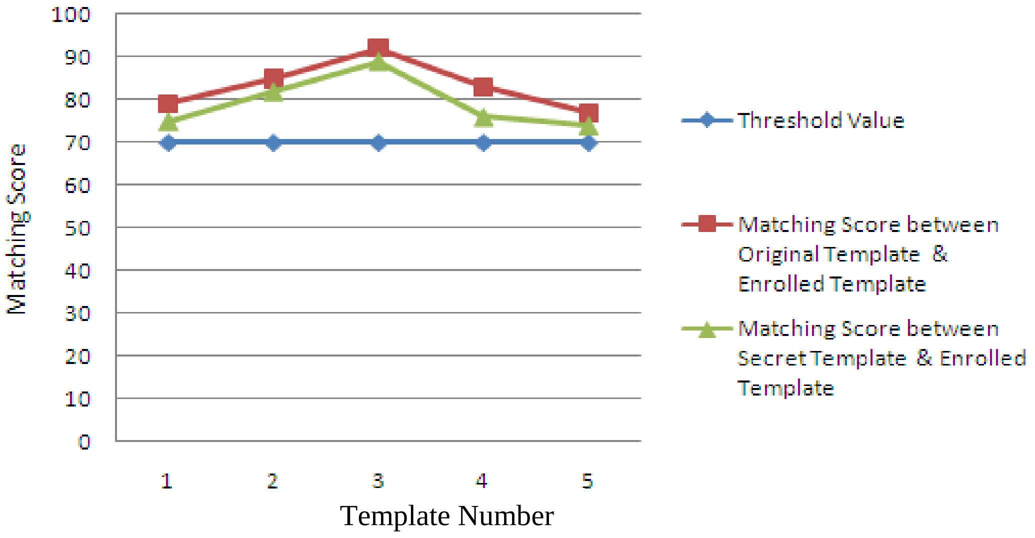
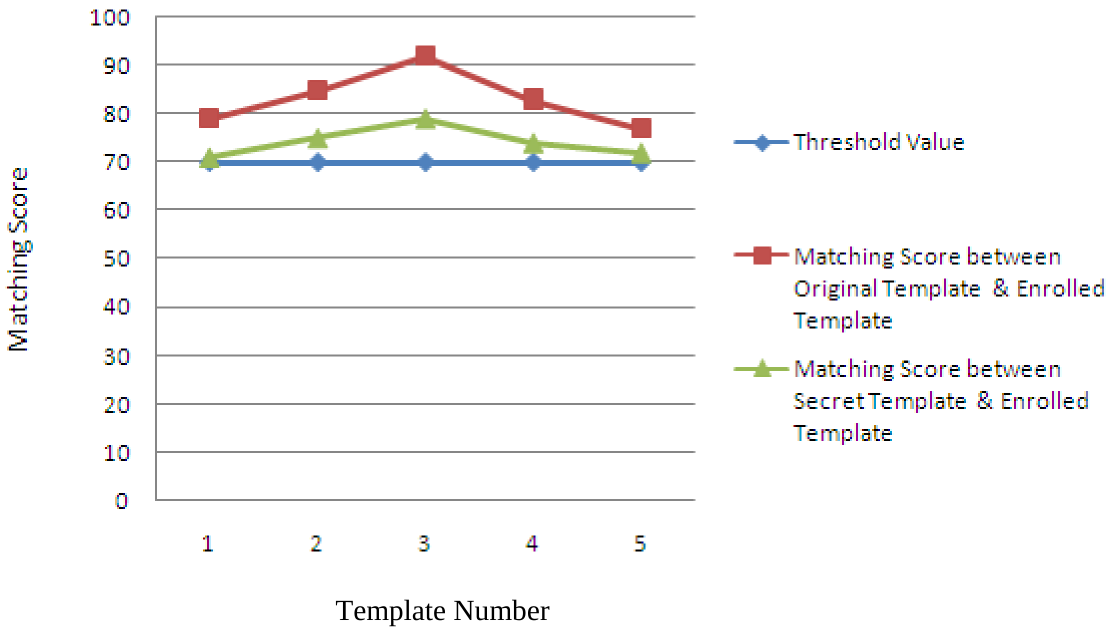


Figure 12.



‘

Figure 13.

*B. Histogram Analysis*

Figure 14 shows the histogram of original template given in Fig 5, Fig 15, Fig 16, Fig 17, Fig 18 gives the histograms of secret templates given in Figure 6, Figure 7, Figure 8 and Figure 9 respectively. Comparing the histograms of original template and secret template, we found that there is very less change in the original template and secret template. As the size of watermark information increases, this change in original template and secret template also increases accordingly.

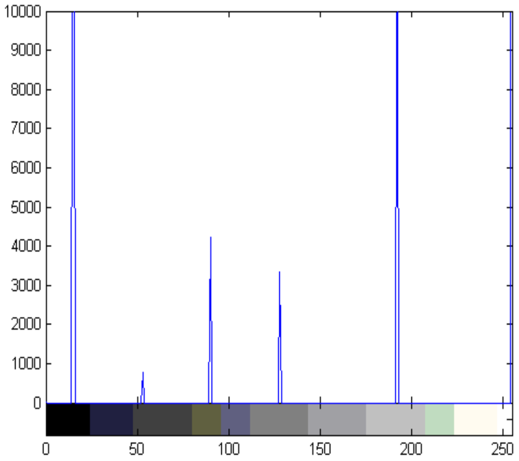


Figure 14. Histogram of original template

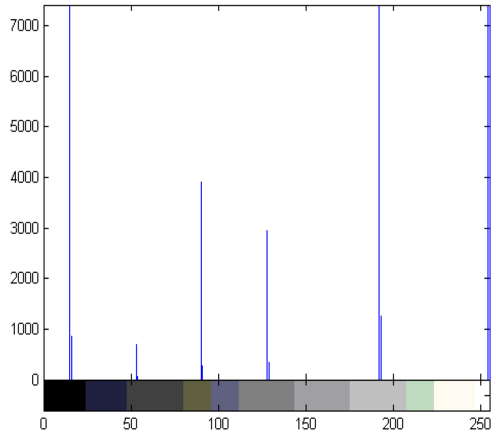


Figure 15. Histogram of original template secret template given in figure 6

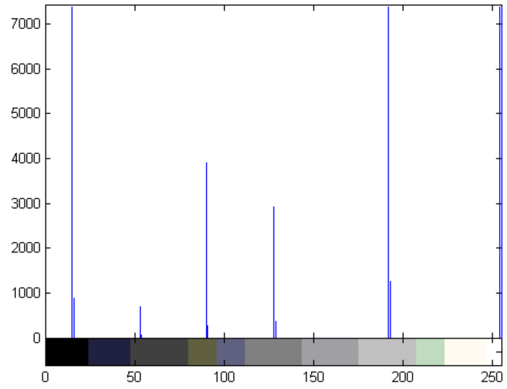


Figure 16. Histogram of original template secret template given in figure 7

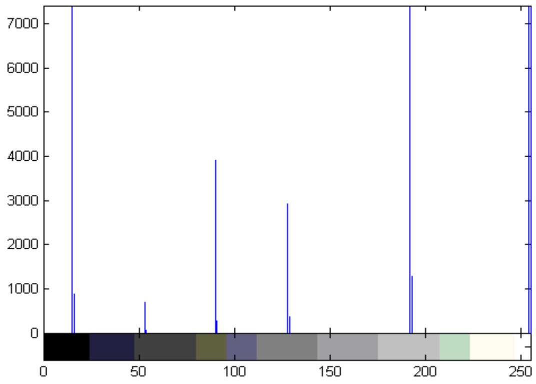


Figure 17. Histogram of original template secret template given in figure 8

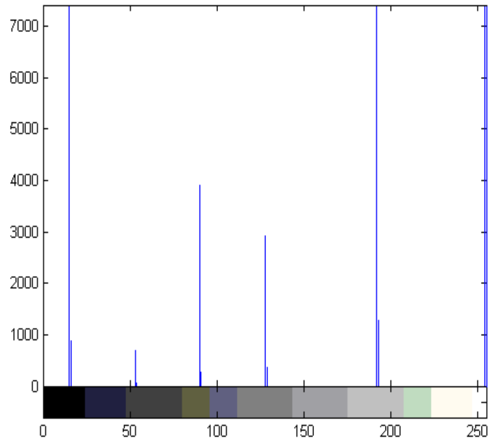


Figure 18. Histogram of original template secret template given in figure 9

## V. Conclusion & Future Work

This work present how watermarking helps in security of biometric template. We showed that watermarking avoids the forging and replacement of biometric template by the attacker. But, this process also increases the responsibility of database manager. Database Manager has to manage the key secretly. In future, we will try to combine watermarking with cryptography techniques and try to increase robustness of biometrics systems. We will also try to prevent other types of attacks on the biometrics systems by using watermarking, cryptography and data hiding techniques.

## References

[1] Schneier, Bruce, "Inside risks: the uses and abuses of biometrics," August 1999 Communications of the ACM, Volume 42 Issue 8.

[2] Rajkumar Yadav, Rahul Rishi & Sudhir Batra, "A New Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.

[3] Parvathi Ambalakat, "Security of Biometric Authentication Systems", 21st Computer Science Seminar, SA1-T1-1.

[4] Jing Dong and Tieniu Tan, "Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations", National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, 10190, Beijing, China.

[5] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proc, IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[6] M. Kutter, F. Jordan, and F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation," Proc. SPIE, vol. 3022, pp. 518-526, 1997.

[7] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT Domain System for Robust Image Watermarking," Signal Processing, vol. 66, no. 3, pp. 357-372, May 1998.

[8] Jain A.K.Ross A and Uludag U. "Biometrics Template security: Challenges and solutions" in *Proc. of* European Signal Processing Conference September 2005.

[9] U.K. Biometric Working Group, "Biometric security concerns," Technical Report, CESG, September 2003, http://www.cesg.gov.uk/site/ast/biometrics/media/ BiometricSecurityConcerns.pdf.

[10] Stallings.W. Cryptography and network security: Principles and practice. In *Prentice Hall*, 2003.

[11] Jain A.K.,Bolle R. and S. Pankanti. Biometrics: Personal identification in networked society. *Norwell, MA: Kluwer*, 1999.

[12] Soutar C.and Roberge. D *et al*. Biometric encryption. *ICSA Guide to Cryptography*, *McGrow-Hill*, 1999.

[13] A. Gutub, M. Faltani, "A Novel Arabic Text Steganography Method Using Letter Points and Extension", WASET International Conference on Computer Information and System Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[14] RJ Anderson, FAP Petitcolas, "On the Limits of Stegnography", IEEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[15] Chandramouli, R., Memon, N.D., 'Steganography capacity: A steganalysis perspective', Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003.

[16] Pal, S.K., Saxena, P.K., Muttoo, S.K., 'Image steganography for wireless networks using the handmaid transform', Internation Conference on Signal Processing & Communications (SPCOM), 2004.

[17] Parvez M. T. and Gutub A., "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[18] Eugene T. Lin and Edward J. Delp, "A Review of Data Hiding in Digital Images", Video and Image Processing Laboratory (VIPER), Indiana.

[19] Schneier, Bruce, "*Inside risks: the uses and abuses of biometrics*," August 1999 Communications of the ACM, Volume 42 Issue 8.

[20] Shenglin Yang, Ingrid M. Verbauwhede, "*A secure fingerprint matching technique*," Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, September 2002.

[21] Uludag. U, Pankanti. S, Prabhakar. S and Jain. A.K, “Biometric Cryptosystems: issues and challenges,” Proceedings of the IEEE, Volume: 92, Issue: 6, June 2004.
[22] Waldmann, Ulrich, Dirk Scheuermann, and Claudia Eckert, “*Protected transmission of biometric user authentication data for oncard-matching,*” Proceedings of the 2004 ACM symposium on Applied computing March 2004.
[23] Williams, John Michael,” *Assurance in life/nation critical endeavours: Biometrics or ... biohazards?*” Proceedings of the 2002 workshop on New security paradigms, ACM Press.\
[24] F Hartung., B. Girod.: Watermarking of uncompressed and compressed video, Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3): 283-301.
[25] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2, JUNE 2008