International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, pp-027-035 ISSN: 2249-6645

Removal of Communication Channel Attack on Biometric Authentication System Using Watermarking

Kamaldeep
Assistant Professor Savera Group of Institutions (Gurgaon)

Abstract — Biometrics authentication system used the physical or behavioral characteristics for identify an individual. With the wide use of biometrics authentication system, the security of biometrics system emerged an important research issue. A biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. In this paper, an approach to enhance the biometrics security by using watermarking technique has been proposed. For hiding the information in the biometrics image taken by sensor, the semi-pixel difference method [1] has been used. In this method, first the pixel is divided into two semi-pixels and their difference is calculated. According to the calculated difference, the watermarked bit is inserted at a pixel value. The pixels for insertion of watermark are selected by using pseudo random number generator which is seeded with a secret key.

After insertion of watermark at sensor module with the help of SPD insertion method it sent to the other end for matching with stored template. The SPD retrieval method finds the watermark. If the watermark is find than the template is original. If the template is tempered by intruder than it is discarded.

Keywords- Biometrics Authentication system, Attacks on biometrcs, Security, Watermarking, Semi-Pixel difference Method etc.

I. INTRODUCTION

A biometrics based authentication system can use physical or behavioral characteristics for identification and verification of a person. It has been deployed in various areas in the industry as well as in military and in the e-commerce. In the current digital world, our biometrics system has a variety of attacks which makes the biometrics system insecure for authentication and communication. With the wide spread utilization of biometrics identification system, establishing the authenticity of biometric data itself has emerged as an important issue. The biometrics system and the attacks on it is shown by the figure 1.

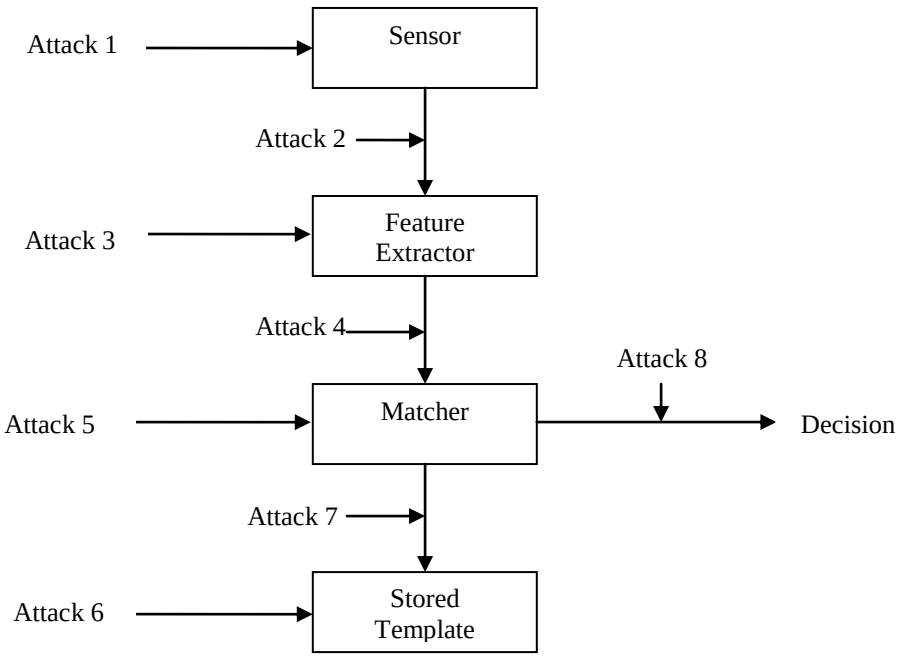

Fig 1. Biometrics authentication system and various attacks on it(Derived from[2])

Digital watermarking or simply watermarking is defined as a process of embedding information like owner name, company logo etc. in the host data. The process of watermark insertion and extraction is given in Figure 2 and Figure 3 respectively [3]. General image watermarking methods can be divided into two groups according to the domain of application of watermarking. In spatial domain methods [4], 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 [5]. Watermarking is very similar to steganography in that both seek to hide information in the Cover-object. However steganography is related to secret point-to-point communication between two parties. Thus, steganography techniques are usually having a limited robustness and protect for the embedded information against modifications that may occur during transmission, like format conversion, compression or A/D conversion. On the other hand, watermarking rather than steganography principles is used whenever the media is available to parties who know the existence of the embedded information and may have interest removing it. Thus, watermarking adds additional requirements of robustness. An ideal watermarking system would embed information that could not be removed or altered without making significant perceptual distortion to the media. A popular application of watermarking is to give a proof of correctness of digital data by embedding copyright statements [6].

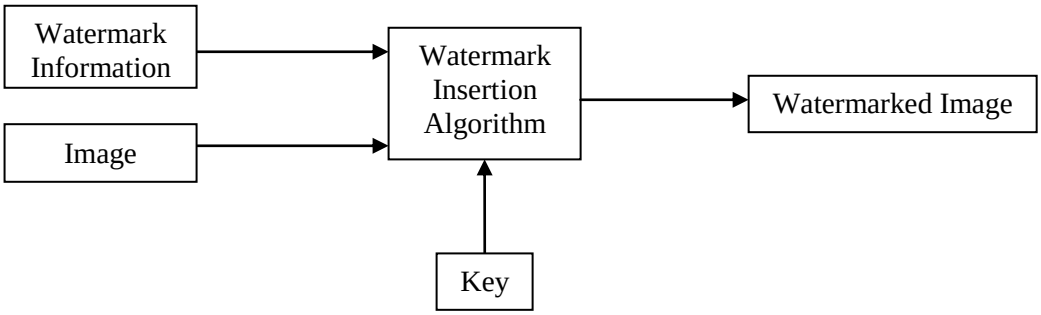

Fig 2. Watermark Insertion Process

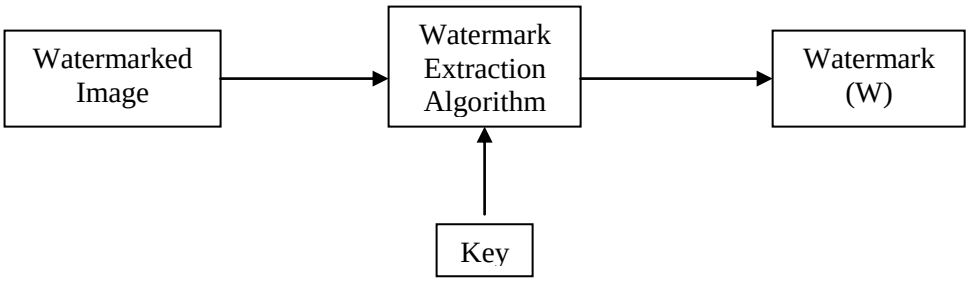

Fig 3. Watermark Extraction Process

The rest of the paper is organized as follows:

In section 2, use of watermarking in biometrics has been discussed. Section 3 gives Attack no-2 on biometrics system. Section 4 indicates the proposed method. The section 5 discusses the semi-pixel difference method of watermarking. Section 6 discusses the result and conclusion, some emphasis on future work.

II. USE OF WATERMARKING IN BIOMETRICS [7]

In many cases, the appropriate use of cryptography also reduces this threat [8]. The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric data before it is transmitted from one physical device to another. Steganography can greatly reduce these attacks because attackers must have to obtain the system's private data in addition, to breaching the security of the capture device or biometric storage. This makes these attacks considerably more difficult to achieve But steganography is more secure than cryptography because there is no separate key in steganography rather key is inbuilt in the template [9].

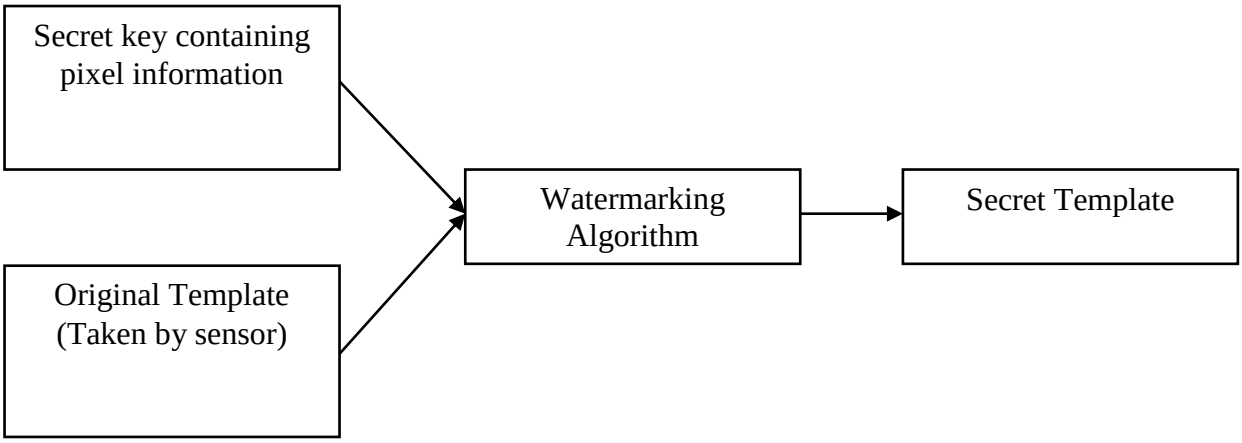

Fig 4. Use of Watermarking in Biometrics

III. ATTACK NO-2 ON BIOMETRICS SYSTEM.

This point of attack is known as "Attack on the channel between the scanner and the feature extractor" or "Replay attack". In this attack, the attacker intercepts the communication channel between the scanner and the feature extractor to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner. The block diagram of biometrics authentication system and the attack no.2 is given by figure 5.

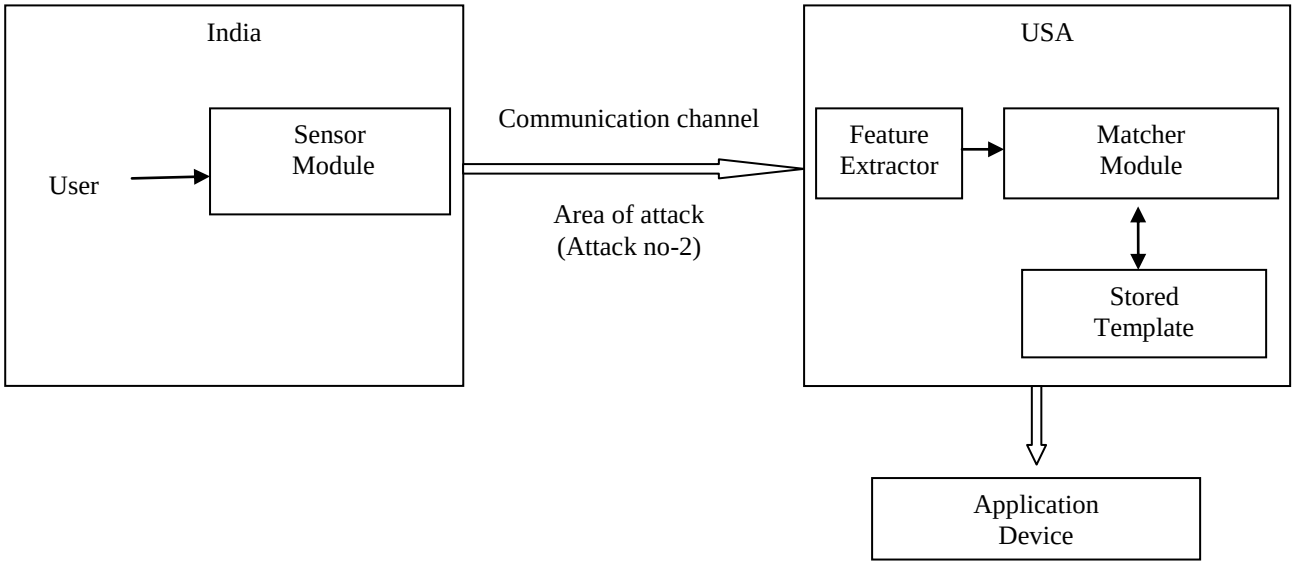

Fig 5. Attack no 2 on the communication channel between sensor module and feature extractor module

IV. PROPOSED APPROACH

In this section, we gave an approach to remove the communication channel attack i.e. No. 2 Attack on biometric system. Suppose the sensor module is present in INDIA and matching module is present in USA. Then the enrolled template is sent out to USA for matching with stored template. In between intruder can manipulate with the enrolled template. By using watermarking we can remove this problem. The watermark text is inserted within the enrolled template to make it secret template. In the first case, if intruder try to tamper with the secret template then it also changes the watermark text which become visible at the retrieval end i.e. (Matching Module Site.). In, the second case, if intruder replace the original enrolled template then it also become clear at the matching module site because in this case watermark information would be missing from the replaced template. So, by using the watermarking technique we can remove the communication channel attack. The proposed scenario is given by the figure 6.

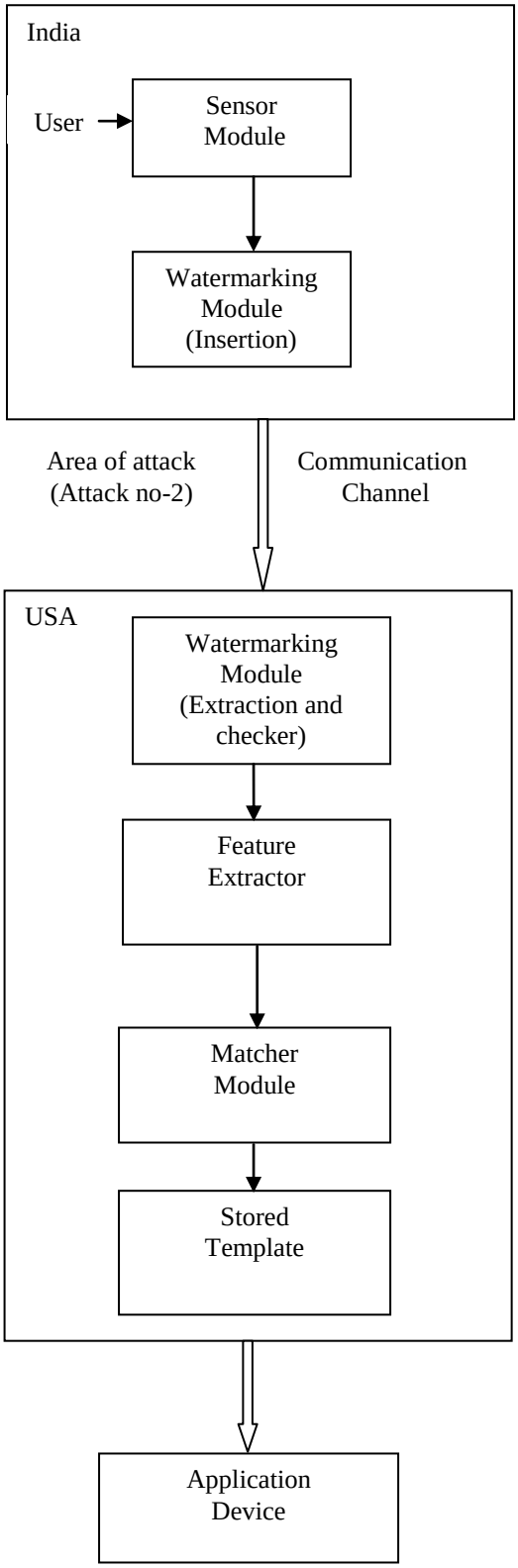

Fig 6. Proposed method for removing the attack no 2 i.e. Attack between sensor and extractor module.

V. SEMI-PIXEL DIFFERENCE METHOD[1]

In this section, watermarking method is described i.e. SPD (Semi-Pixel Difference) method for hiding watermark information in the spatial domain of the gray scale image i.e. biometrics image. SPD method first divides each pixel into two semi pixels known as semi-pixel 1 and semi-pixel 2 and then watermark information is inserted at the pixel value according to the difference of semi-pixel 1 and semi-pixel 2. If we want to insert watermark bit 0 at a pixel value, then the difference of semi-pixel 1 and semi-pixel 2 must be an even number. Otherwise, we made the semi-pixel difference equal to the even number by adding or subtracting 1 to the pixel value. Similarly, if we want to insert watermark bit 1 at a pixel value, then semi-pixel difference must be an odd number otherwise we made the semi pixel difference equal to odd number by adding or subtracting 1 to the pixel value. The pixels for insertion of watermark information are selected by using Pseudo-Random Number Generator that is seeded with a secret key. The split process of pixel is shown in Figure 7. Table I shows how watermark bits can be inserted according to the Semi-Pixel Difference. Figure 8 shows the watermark insertion process & Figure 9 shows the watermark extraction process.

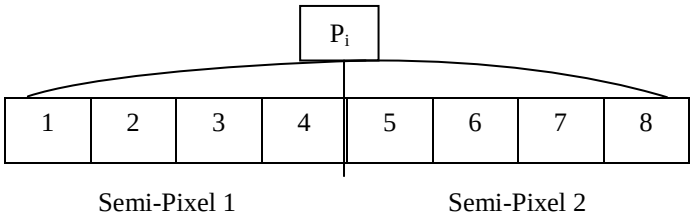

Fig 7. Split Process

Table I: Watermark Insertion according to the Semi-Pixel Difference.

Semi-Pixel Difference	Watermark Bit to be Embedded
0	0
1	1
2	0
3	1
4	0
5	1
6	0
7	1
8	0
9	1
10	0
11	1
12	0
13	1
14	0
15	1

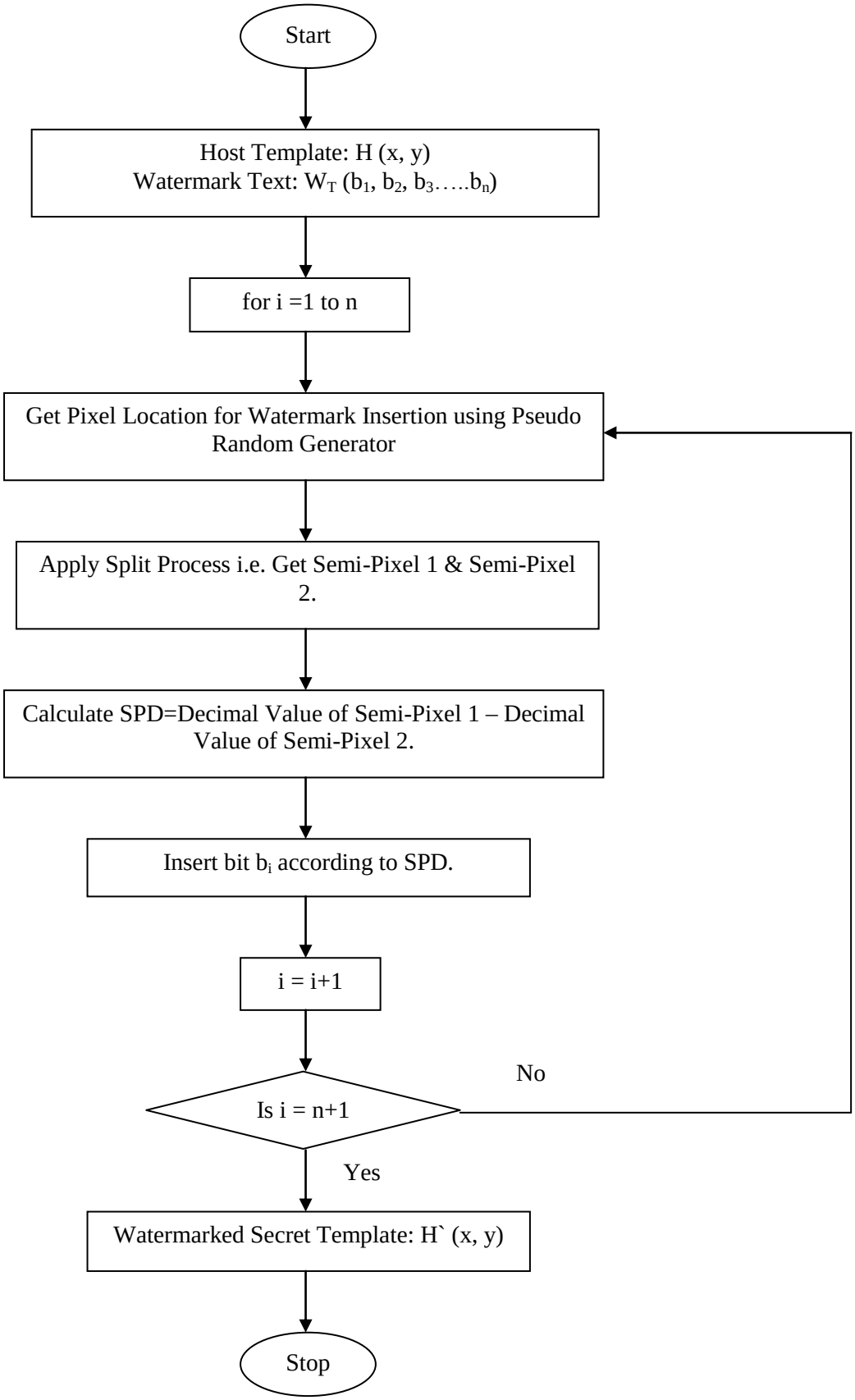

Fig 8. Watermark Insertion Process

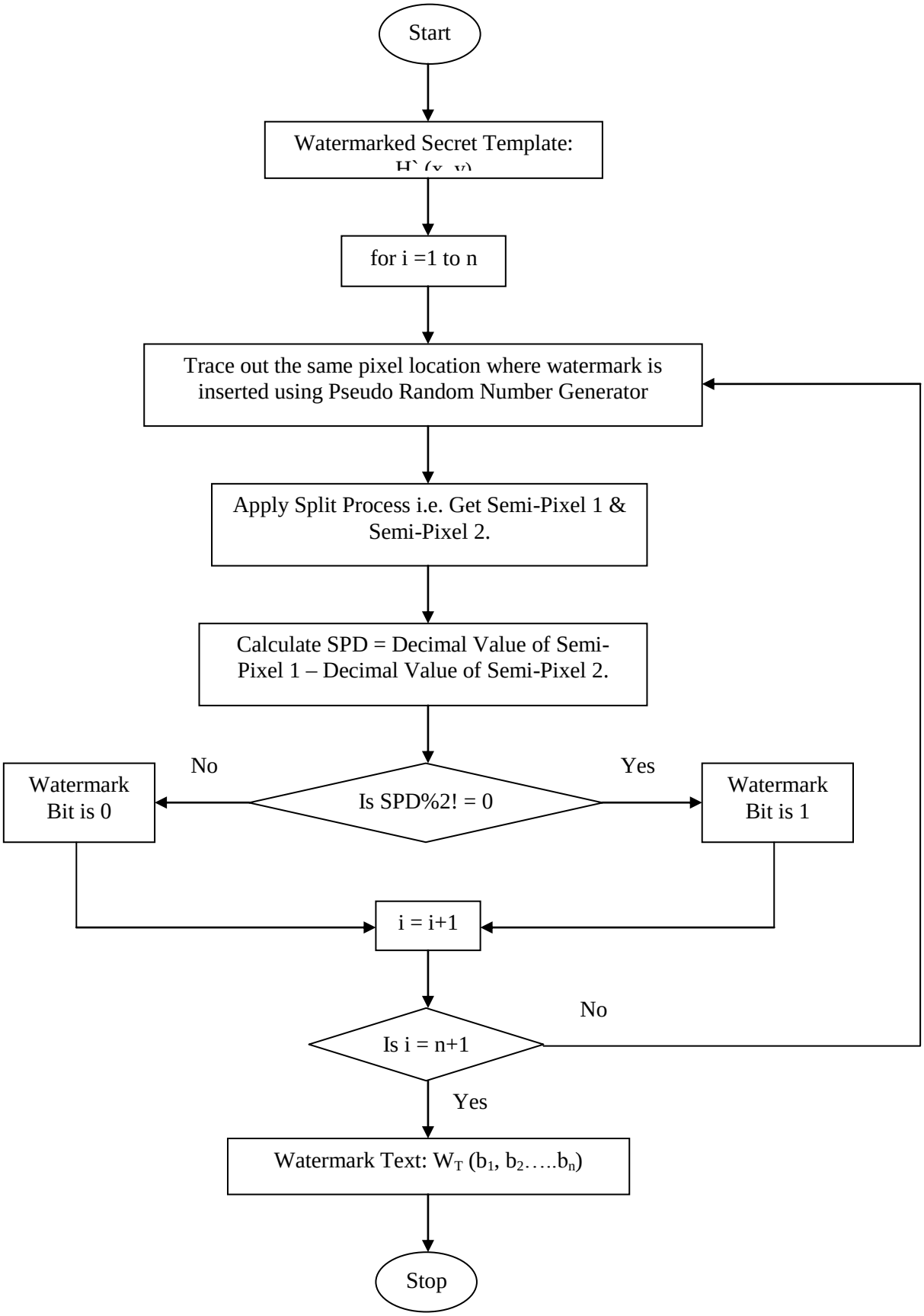

Fig 9. Watermark Extraction Process

5.1 Insertion Algorithm

Step 1: Read the host template: H(x, y)
Step 2: Read the watermark text: $W_T(b_1, b_2, \ldots\ldots b_n)$.
Step 3: for i=1to n.
Step 4: Get pixel location P_i for insertion of watermark information using pseudo random number generator.
Step 5: Apply split process i.e. split the pixel into two equal parts i.e. semi –pixel 1 and semi-pixel 2
Step 6: Calculate d_1 and d_2 using equation (1) and (2) respectively.
d_1=DEC (semi-pixel1) ---------- (1)
d_2=DEC (semi-pixel2) ---------- (2)
Step 7: Calculate SPD using equation (3).
SPD=Abs (d_1-d_2) ---------- (3)
Step 8: Calculate Decision Variable (DV) using equation (4).
DV=SPD Mod 2---------- (4)
Step 9: If b_i=0 than go to step 10 else go to step 11.
Step10: (a) If DV = = 0, then b_i is present at P_i.
(b) If DV! = 0, then add or subtract 1 to P_i such that DV becomes equal to 0 and insert b_i.
Step11: (a) If DV! = 0 then b_i is present at P_i.
(b) If DV = = 0, then add or subtract 1 to P_i such that DV becomes equal to 0 and insert b_i.
Step 12: Go to step (3)
Step 13: Watermarked secret template: H`(x, y).
Step 14: END.

5.2 Extraction Algorithm

Step 1: Read the watermarked secret template: H`(x, y)
Step 2: for i=1to n.
Step 3: Trace out the same pixel location P_i using pseudo random number generator where watermark information is present.
Step 4: Apply split process i.e. split the pixel into two equal part i.e. semi –pixel 1 and semi-pixel 2
Step 5: Calculate d_1 and d_2 using equation (1) and (2) respectively.
Step 6: Calculate SPD using equation (3).
Step 7: Calculate Decision Variable (DV) using equation (4).
Step 8: If DV = = 0, then 0 is the watermark bit else 1 is the watermark bit.
Step 9: Go to step (2).
Step 10: Collect the entire watermark bits to get the watermark text: $W_T(b_1, b_2, \text{------}b_n)$.
Step 11: END

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we gave an approach to show that how communication channel attack can be removed by using invisible watermarking. For insertion of the watermark we used the semi – pixel difference method. The watermarked template is sent to matching module which is present abroad. The watermark is extracted at the matching module site and at that site secret template is checked for its validity by using the extracted watermark. In future, we will try to improve the security of biometrics further by using data hiding techniques and cryptography.

References

[1] yadav,R.K.; chawla,G and Saini, R, "Semi Pixel Difference Method For Digital Image Watermarking With Minimum Degradation In Image Quality"
[2] Jain, A.K.; Uludag, U., "Hiding biometric data", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.
[3] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," Proc, IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.
[4] M. Kutter, F. Jordan, and F. Bossen, "Digital Signature of Color Images Using Amplitude Modulation," Proc. SPIE, vol. 3022, pp. 518-526, 1997.
[5] 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.

[6] Mikdam A. T. Alsalami and Marwan M. AL- Akaidi," Digital Audio Watermarking"

[7] Kant,C;Nath,R;and chaudhary,S"Biometrics Security using Steganography" International Journal of Security, Volume (2) : Issue (1),2008

[8] Soutar C., "Biometric system security," White Paper, Bioscrypt, http://www.bioscrypt.com..2004

[9] Uludag U., Pankanti S., Prabhakar S., and Jain A. K., "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE, vol. 92, no. 6, pp. 948–960, 2004.

[10] Jain, A.K., Bolle, R., and Pankanti S.,"Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999.

[11] Jain A. K., Ross A., and Prabhakar S., "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[12] Maltoni D., Maio D., Jain A. K., and Prabhakar. S. Handbook of Fingerprint Recognition. Springer, New York, 2003.

[13] Jain, A.K., Uludag, U., "Hiding biometric data", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.

[14] Jain, A.K., Uludag, U., "Hiding biometric data", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 25, Issue: 11, Nov. 2003.

[15] Ratha N. K., Connell J. H., and R. M. Bolle. An analysis of minutiae matching strength. In Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pages223.

[16] Ratha, N.K., Connell J.H., and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3, 2001.

[17] Waldmann, Ulrich, Dirk S., and Claudia E., "Protected transmission of biometric user authentication data for on card-matching," Proceedings of the 2004 ACM symposium on Applied computing March 2004.

[18] Jain, Anil K. and Arun Ross, "Multibiometric systems," Communications of the ACM," January 2004, Volume 47,Number 1 (2004).

[19] Anil. K., Ross A., and Prabhakar S., "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[20] Ratha, N.K., Connell J.H., and R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3, 2001.

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