NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 5, ISSUE 5, May-2018

EFFICIENT REVERSIBLE WATERMARKING TECHNIQUE FOR PROTECTED TEMPLATES OF BIOMETRIC AUTHENTICATION SYSTEM

MRS. S. D. SHINDE
M.E. Student, Department of Electronics Engineering, WIT, Solapur, India.
itsashraddha@gmail.com

MR. P.S. MALGE
Asst. Professor, Department of Electronics Engineering, WIT, Solapur, India
p_malge@yahoo.com

ABSTRACT
This paper describes an efficient technique of reversible watermarking for protected templates of biometric authentication system. Tag based searching is used in authentication that reduces searching time. RST invariant features of fingerprint image are used to crate tag. Whirlpool hash method is used to generate hash code which is further used as watermark embedded in biometric fingerprint image. This technique improves speed of verification. This technique improves security of biometric authentication system.

KEYWORDS: reversible watermarking, tag, RST, hash code, whirlpool hash etc.

I. INTRODUCTION

Uniqueness of the biometric features plays important role in fingerprint authentication system. The digital transmission of biometric data considered as flexible and cost effective communication models. But most important drawback of it is, such data may be duplicated very easily without introducing any quality degradations to the content. Digital watermarking technique is used to resolve this problem. This does not allow anonymous users to access unauthentic information without owner's permission. Any anonymous person can access the system if the database of templates has been tampered. This unauthentic biometric data can compromise the authentication system. Every human user has a limited number of biometric traits and hence for security reasons stolen traits cannot be reused for authentication.
Thus, revocability of a fingerprint data is a serious problem for any biometric authentication system. To solve this problem, it is necessary to authenticate the protected templates stored in a database.
There are many techniques of template protecting introduced to impart revocability to biometric traits. These techniques are categorised as feature transformation based techniques and biometric crypto system. In feature transformation methods, unprotected biometric features transformed by using key specific transform function that used to generate protected template, which is then stored in database. At the time of verification, query biometric features are transformed by using identical key and by a specific transform function. It is then matched with the database protected templates. These types of authentication systems can be spoofed easily by using stolen protected template.
In order to make security of protected templates strong, an efficient reversible watermarking technique with tag based searching is proposed. It improves the speed of verification and security.

II METHODOLOGY

A. Enrollment Process

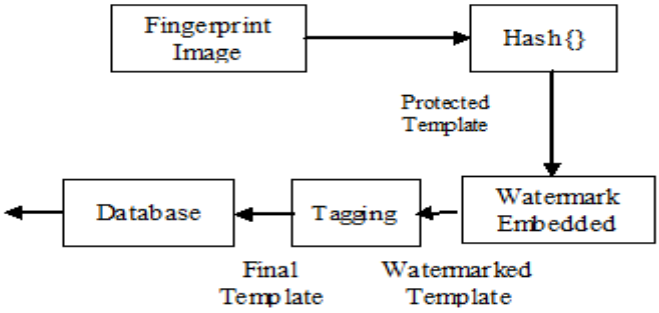

Figure 1: User Enrollment Process in Biometric

AUTHENTICATION SYSTEM

A. STEPS IN ENROLLMENT PROCESS:

a) Select fingerprint image from database.

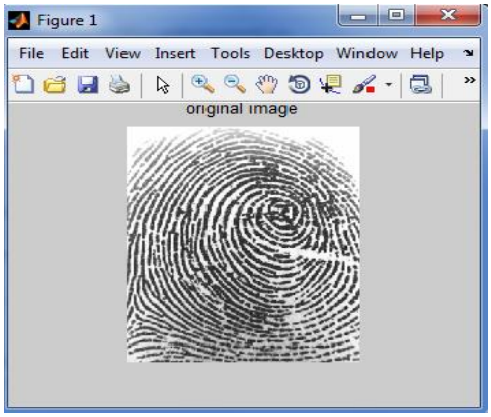

Figure 2: Fingerprint Image for Enrolment

b) RST features of the fingerprint image are calculated as:

i) Rotation: The new coordinates of a point in the x-y plane rotated by an angle θ around the z axis. Here (x,y)= T {(a,z)},
Where, T is the rotation transformation.
x = acos θ - zsin θ
y = asin θ + zcos θ

ii) Scaling: If x-coordinate of every point multiplied by positive constant Sx, then this transformation expand or compress every plane figure in x-direction. Here T is scaling transformation.
x = Sxa
y = Syz

iii) Translation: A translation is used as vector T = (Tx, Ty) and transformation of coordinates is used as
x = a + Tx
y = z + Ty

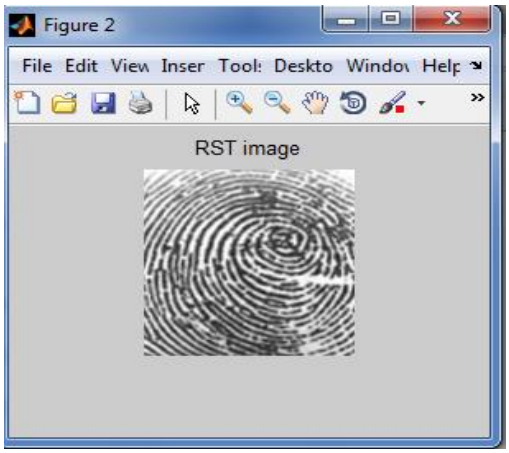

Figure 3: RST Image

c) Tag is calculated from entropy of rst fingerprint image by using formula:

Entropy= $\sum_i P_i \text{Log}_2 P_i$

Where, P_i is probability that difference between two adjacent pixels is equal to i, and Log_2 is base 2 logarithm.

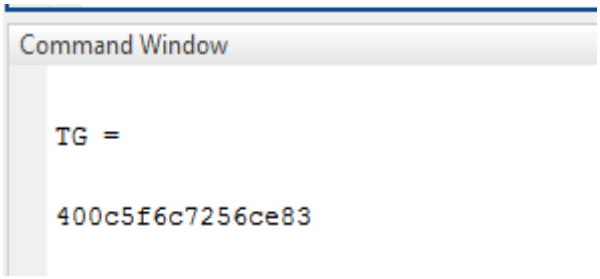

Figure 4: Tag Output Window

d) Tag is stored into database.

e) Whirlpool hash algorithm is used to generate 512 bit digest from input fingerprint image.

f) Whirlpool hash algorithm:

1) The algorithm use an input image with a maximum length of bits in image less than 2^256 bits and it produce an output as 512-bit message digest.

The input value is processed in the form of 512-bit blocks.

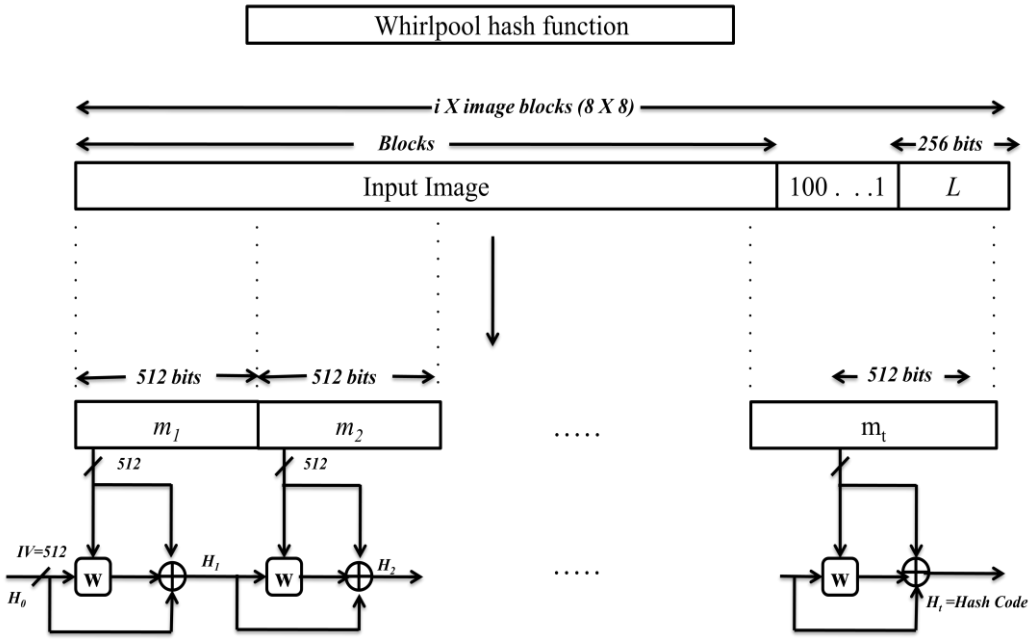

Figure 5: Block Diagram of Hash Algorithm

The processing of input consists of following steps:

Step 1: Append the padding bits:

The message padded .Padding bits in the range of 1 to 512.The padding contain single 1-bit and number of 0-bits

Step 2: Append length.

256 bits of block is appended to the message. This block is unsigned 256-bit integer.

Step 3: hash matrix initialization.

The hash Hi is an 8X8 matrix.

It is used to hold intermediate and final value of hash function. The matrix is initialized as zero matrix.

Step 4: Output of hash algorithm is 512 bits.

g) Reversible watermarking technique is used to watermark whirlpool hash in the fingerprint image and produce watermarked fingerprint image

EMBEDDING ALGORITHM

Insert binary hash code into fingerprint image by following method:

1) Calculate difference between twice of each pixel value and value of adjacent pixel of image up to size of image.

2) If this difference is more than 1 and below than 255 and adjacent pixels value are not odd then embed 1 at lsb of first pixel and watermark bit at lsb of second pixel

3) Otherwise embed 0 at lsb of first pixel and watermark bit at lsb of second pixel.

4) If this difference is less than 1 and more than 255 then no change in pixel values.

6) After embedding data into image, watermarked image store into database.

Figure 6: Watermarked Image

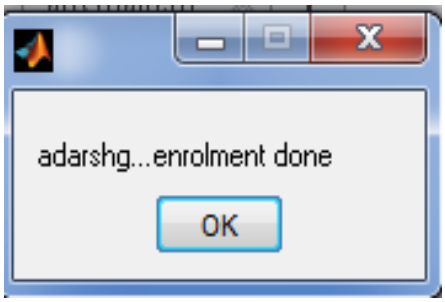

Figure 7: Enrolment Done

B. VERIFICATION PROCESS

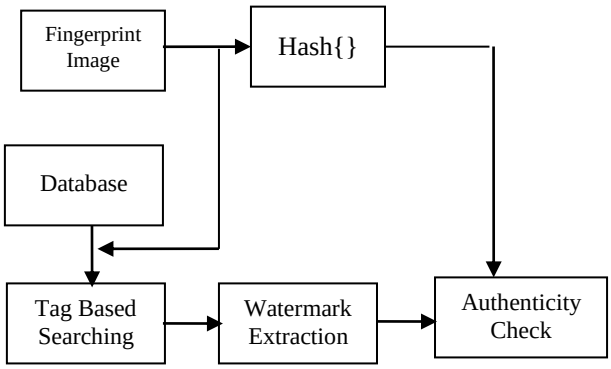

Figure 8: Verification Process for Biometric Authentication System

a) Take Query fingerprint image from database which is not enrolled, used for verification process.

Figure 9: Query Fingerprint Image

a) RST of query fingerprint image is calculated

Figure 10: RST of Query Fingerprint Image.

b) Calculated RST features and entropy of query fingerprint image from this tag is created.
c) This tag is used for tag base searching.
d) Tag of query fingerprint image and tags stored in database is matches.
e) If tag is matched then Hash code is generated from query fingerprint image to produce hash code of the query fingerprint image.

Figure 11: Tag is matched

f) Take watermarked image from database and extract watermark by following process:
1) Read adjacent pixels of watermarked image.
2) Set lsb of both the pixels to 1.
3) Calculate difference between twice of each pixel and adjacent pixel of image up to size of image.
4) If this difference is more than 1 and below than 255 then multiply lsb of first pixel by 1.
5) If lsb of first pixel is 1 then
5.1) multiply lsb of second pixel by one and this lsb value is watermarked bit.
5.2) set lsb of first pixel to 0 , we get first pixel of original image.
5.3) set lsb of second pixel to 0 , we get second pixel of original image.
6) If lsb of first pixel is 0 then
6.1) multiply lsb of second pixel by one and this lsb value is watermarked bit.
6.2) set lsb of first pixel to 1, we get first pixel of original image.
6.3) set lsb of second pixel to 1, we get second pixel of original image.
7) After watermarked extraction, we get hash code.
8) Compare hash code of watermarked image with hash code of query image and its matching score is more than and equal to threshold value then person is authenticate otherwise unauthorized person and verification is done.

Figure 12: Verification Massage

Table1. Average BER for Different Attacks on Watermarked Fingerprint Image

Attacks	Average BER of Samples
No attack	0.00
Gaussian Noise	0.5442
Blur	0.4687
Rotation	0.4859

IV. CONCLUSION

To solve problem of security of protected template, reversible watermarking technique is proposed and it is implemented on biometric authentication system. This technique enhanced security of biometric authentication system. To check authenticity and reduce burden on biometric authentication system a tag based searching is used. Applied tag based searching improved speed of verification.

V.ACKNOWLEDGMENT

I would like to seize the opportunity to express my sincere gratitude towards Head of Department Prof. S.R. Gengaje, project guide Prof. P.S. Malge and other electronics department faculties for their valuable co-operation and guidance.

VI. REFERENCES

I. D.M. Thodi, J.J. Rodriguez, Prediction-error based reversible watermarking, In: International Conference on Image Processing, 2004, pp. 1549–1552.
II. G. Xuan, C. Yang, Y. Zhen, Y.Q. Shi, Z. Ni, Reversible data hiding using integer wavelet transform and companding technique, Lecture Notes in Computer Science, Digital Watermarking, vol. 3304, 2005, pp.115–124, Springer Berlin Heidelberg
III. Hui-Rong Wang (2008), A Novel Discrete Wavelet Transform Based Digital Watermarking Scheme, 2nd International Conference on Anticounterfeiting, Security and Identification ,pp 55-58.
IV. H.W. Tseng, C.P. Hsieh, Prediction-based reversible data hiding, Information Sciences 179 (14) (2009) 2460–2469.
V. J. Lee, Y. Chiou, J. Guo, S. Member, Reversible Data Hiding Based on Histogram Modification of SMVQ Indices, IEEE Transactions on Information Forensics and Security 5 (4) (2010) 638–648.
VI. J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems 13 (8) (2003) 890–896.
VII. L.T. Ko, J.E. Chen, Y.S. Shieh, H.C. Hsin, T.Y. Sung, Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems, Computational and Mathematical Methods in Medicine 2012 (2012) 1-8.
VIII. M.J. Saberian, M.A. Akhaee, F. Marvasti, An invertible quantization based watermarking approach, In: IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas,USA,2008, pp.1677–1680.
IX. Noore, A., Singh, R., Vatsa, M. and Houck, M.M. (2009) Enhancing security of fingerprints through contextual biometric watermarking, Forensic Science International Vol. 169, Issue 2, Pp. 188-194
X. P.Tsai, Y.-C. Hu, H.-L. Yeh, Reversible image hiding scheme using predictive coding and histogram shifting, Signal Processing 89 (6) (2009) 1129–1143.
XI. Tudoroiu, I. Caciula, D. Coltuc, Block map implementation of difference expansion reversible watermarking, In: 10th International Symposium on Signals, Circuits and Systems, 2011, pp. 1–4.
XII. Uludag, U., Gunnsel, B. and Ballan, M. (2001) A spatial method for watermark of fingerprint images, Proceedings of. First International Workshop on Pattern Recognition in Information Systems, Setúbal, Portugal, Pp. 26-33.

XIII. V. Sachnev, H.J. Kim, J. Nam, S. Suresh, Y.Q. Shi, Reversible watermarking algorithm using sorting and prediction, IEEE Transactions Circuit and Systems for Video Technology 19 (7) (2009) 989–999.
XIV. WILLIAM STALLINGS,The Whirlpool Secure Hash Function Cryptologia, 30:55–67, 2006ISSN: 0161-1194 DOI: 10.1080/01611190500380090
XV. Zebbiche, K. and Ghouti, L. et al. (2006) Protecting fingerprint data using water marking. First NASA/ESA Conf. on Adaptive Hardware and Systems (AHS‟06), Pp.451–456