Biometric Authentication System using Reversible Watermarking Technique: Overview

Mrs. S. D. Shinde[1] Mr. P.S. Malge[2]
[1]ME Student [2]Assistant Professor
[1,2]Department of Electronics Engineering
[1,2]WIT, Solapur, India

Abstract— The proposed work describes a mechanism of reversible watermarking technique to enhance the security of biometric authentication system. A tag based template searching in reversible watermarking technique is used to check authenticity and reduce burden on biometric authentication system. To create tag rotation, scale and translation (RST) invariant features of biometric image are used. Watermark reversibility in the proposed method will not affect native biometric authentication.

Key words: Reversible Watermarking, Tag, Template, RST

I. INTRODUCTION

Now a day's, compared to a classical authentication mechanisms (ID cards, password, etc.) biometric authentication systems are becoming popular due to uniqueness of the biometric features. The digital transmission of biometric data has introduced flexible, cost effective communication models that are beneficial in various transactions. At the same time, they also possess some serious drawbacks that digital data can be duplicated very easily without introducing any quality degradations to the content. Digital watermarking technique is used to solve this problem. This does not allow an individual, other than the owner, to manipulate, duplicate, or access media information without owner's permission. An unauthentic person gains access to a system (false positive) if the database has been tampered. Thus, the stolen biometric data compromise biometric authentication system. Moreover, every human has a finite number of biometric traits, and for security reasons stolen biometric traits cannot be reused for authentication.

Therefore, revocability of a biometric data is a major challenge for any biometric authentication system i.e. it is essential to authenticate the protected template in a database.

A number of template protecting techniques have been proposed to impart revocability to the biometric traits. These techniques are broadly classified as feature transformation based methods and biometric crypto system. In feature transformation techniques, unprotected biometric features are transformed using key specific transform function to generate protected template, which is then stored in the database. At the time of verification, query biometric features are similarly transformed using identical key; by a specific transform function; and then matched with the stored protected template. The security of feature transformation based techniques relies on the protected template. Therefore, such biometric authentication system can be easily spoofed by applying stolen protected template at the vulnerable point. This type of malicious manipulation is termed as replay attack. In the biometric crypto system, user specifies a secret key and uses it along with the biometric features to generate helper data. The key and helper data are stored in the database as the protected templates. At the time of verification, helper data and the input query biometric data is used to generate a secret key which is matched with the stored secret key.

There are some techniques such as singular value decomposition (SVD), least significant bit (LSB) based watermark embedding technique to validate the database. Salient region-based watermarking can be used for the database protection. There are fragile watermarking techniques to check integrity of the biometric database. However, these watermarking techniques are irreversible and therefore not useful for validating integrity of the protected templates.

In order to secure the database and to check authenticity of the database, a reversible watermarking technique for protected templates along with tag based template searching is proposed. It will reduce search complexity as well as the burden on the biometric authentication system.

II. LITERATURE REVIEW

Uludag proposed watermarking methods that preserve the quantized gradient orientations at and around watermark embedding locations and singular points in the fingerprint image.[1] Noore later on proposed a digital watermarking technique using face and demographic text data as multiple watermarks for protecting the integrity of a fingerprint image.[2] Zebbiche proposed another method using watermarking to protect fingerprint data. They introduced an application of wavelet-based watermarking method to hide the fingerprint minutiae data in fingerprint images.[3] Hui used spatial domain and DCT domain of multi-bits embedded watermark methods, to embed and extract information of the fingerprint characteristics.[4]

Xuan et al. developed a reversible watermarking technique using companding function on integer wavelet coefficients. Companding function is used to compress the coefficients whose values are greater than certain threshold. This process results in an increase in the embedding capacity.[5]. Tsai et al. proposed Histogram Modification Based Reversible Watermarking .The difference between a basic pixel and every other pixel in the block is used rather than the difference of adjacent pixels. However, the prediction method used is less accurate [6]

Saberian et al. presented a Weighted Quantization Method (WQM) approach of reversible watermarking, which can be applied in spatial as well as transform domain. In contrast to other approaches, the distortion caused by this scheme is not payload dependent. It is shown that WQM gives high embedding capacity, when applied to Point to Point Graph (PPG) transform. [7] Lee et al. proposed a

vector quantization based reversible watermarking technique using histogram modification to achieve high embedding capacity.[8] Ko et al. developed a nested QIM watermarking algorithm for medical image watermarking systems, which ensures the recovery of cover image[9].

Tian presented a novel approach, named difference expansion (DE). It gave a new direction to the reversible watermarking methods. It achieves high embedding capacity and low computational complexity compared to the preceding techniques. Several improved DE based watermarking schemes were then proposed over the time [10]. One of the illustrious extension to the DE scheme is the prediction-error expansion (PE), proposed by Thodi et al. [11].Tseng et al. reported a simple reversible watermarking approach based on prediction-error that utilizes values of two pixels in the prediction process of each pixel. Three cases are considered in the embedding procedure. [12] Sachnev et al. reported a PE based algorithm using sorting mechanism. For estimation of the pixels, a rhombus pattern prediction is introduced.[13] Tudoroiu et al. presented a block map based implementation using 7 overlapping blocks. MED is used in prediction process. [14]

III. METHODOLOGY

Plan of proposed work can be divided into following processes:

A. Enrollment Process

1) In the first step of proposed research work RST invariant features of fingerprint image are calculated.
2) Based on the calculated RST features tag is created. Tag is stored into database.
3) Whirlpool hash algorithm is used to create protected template from fingerprint image.
4) Reversible watermarking technique is used to insert protected template in the fingerprint image which will create final protected template.
5) Final Protected template is then stored in the database during the enrollment process.

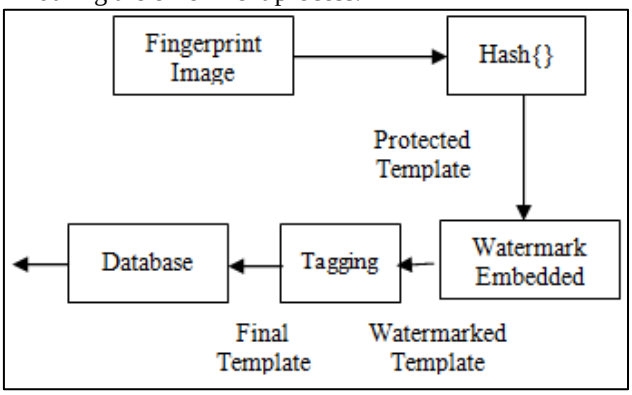
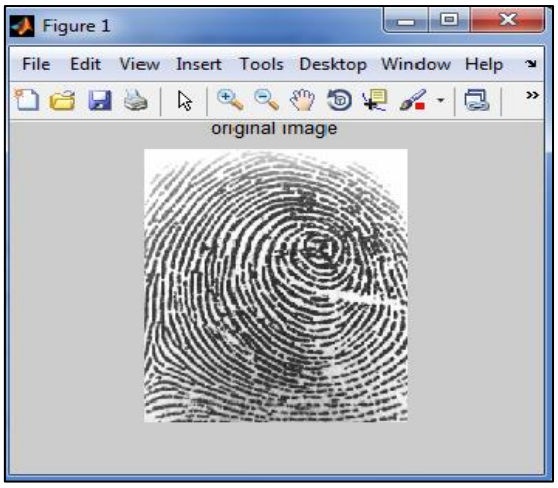


Fig. 1: User Enrollment Process in Biometric Authentication System



Output Window 1: Input Fingerprint Image

Output Window 2: RST Image

Output Window 3: Watermarked image

Output Window 4: Enrolment done

B. Verification Process

Query fingerprint image will be used for verification process.

1) RST invariant features of query fingerprint image is calculated
2) Based on the calculated RST features tag is created.
3) This tag is used for tag base searching.
4) If tag is matched then Hash algorithm is applied on the query fingerprint image to produce protected template i.e. hash code of the query image.
5) Protected template from database is retrieved using watermark extraction.
6) Finally protected template of query fingerprint image is matched with retrieved protected template of watermarked image.
7) Authentication is successful if protected template of query fingerprint image is matched with retrieved protected template of watermarked image

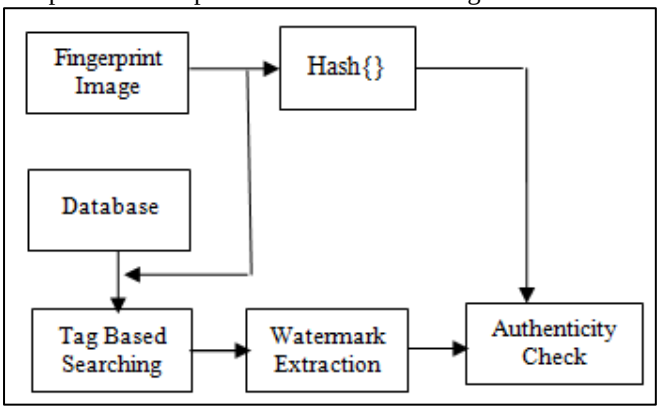
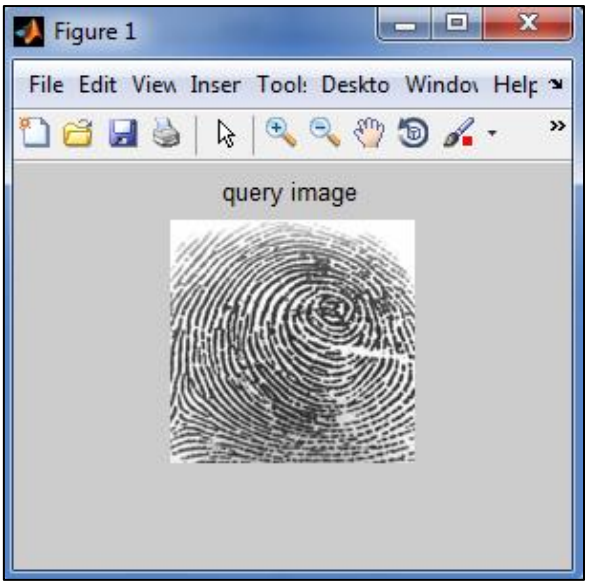
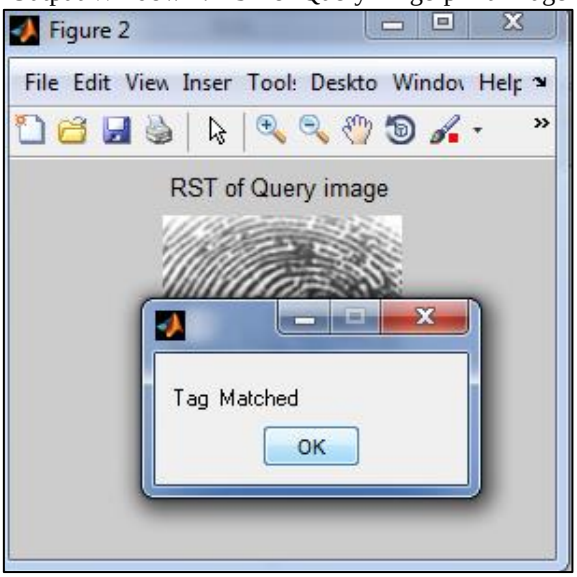


Fig. 2: Verification Process for Biometric Authentication System



Output Window 1: Query Fingerprint Image

Output Window 2: RST of Query Fingerprint Image



Output Window 3: Tag is matched

IV. CONCLUSION

Reversible watermarking technique for protected biometric template is proposed. Proposed reversible watermarking method will generate security layer on top of biometric authentication system which will not affect native biometric authentication accuracy. A tag based template searching in reversible watermarking technique will check authenticity and reduce burden on biometric authentication system.

ACKNOWLEDGMENT

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

REFERENCES

[1] 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.
[2] 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
[3] 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
[4] Hui-Rong Wang (2008), A Novel Discrete Wavelet Transform Based Digital Watermarking Scheme, 2nd International Conference on Anticounterfeiting, Security and Identification ,pp 55-58.
[5] 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
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] J. Tian, Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems 13 (8) (2003) 890–896.
[11] D.M. Thodi, J.J. Rodriguez, Prediction-error based reversible watermarking, In: International Conference on Image Processing, 2004, pp. 1549–1552.
[12] H.W. Tseng, C.P. Hsieh, Prediction-based reversible data hiding, Information Sciences 179 (14) (2009) 2460–2469.
[13] 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.
[14] 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.

