INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 466-472

Impact Factor : 5.725

SECURED INFORMATION TRANSMISSION USING BIOMETRICS

P. Dineshkumar[1], S. Ponharidharsini[2], M. Naveena[3], Roobika R[4], L. Sowmiya[5]

[1]Assistant Professor , Department of Computer Science and Engineering Vivekanandha College of Technology for Women, Tiruchengode, Namakkal-637205, Tamil Nadu, India.

[2,3,4,5]Student, Department of Computer Science and Engineering Vivekanandha College of Technology for Women, Tiruchengode, Namakkal-637205, Tamil Nadu, India.

DOI: https://www.doi.org/10.58257/IJPREMS31211

ABSTRACT

Nowadays, signal processing in the highly encrypted domain has attracted considerable research in interest. Practical cancelable biometrics (CB) schemes must satisfy the requirements of non-invertibility, revocability, and non-linkability without deteriorating the matching accuracy of underlying biometric recognition system. To bridge gap between theory and practice, it is so important to verify that new CB schemes can achieve a balance between conflicting goals of security and matching accuracy. This project investigates security and accuracy trade-off of the newly proposed local ranking-based cancelable biometrics (LRCB) scheme to protect iris-codes. Biometric technologies are being increased and used in the wide variety of applications like border control, authentication systems and health-care applications due to their efficiency, usability, and reliability. As an effective and popular means to protect privacy of image data, encryption thus converts ordinary signal into unintelligible data, so that traditional signal processing usually happens before encryption or after decryption. This project develops secured information transmission using biomatric system. Here, the content owner encrypts original uncompressed image using an encryption key. Then, data-hider updates least significant bits of encrypted image using the data-hiding key for creating a sparse space to accommodate some additional data. So Iris image of person cannot duplicated for other. With an encrypted image containing additional data, if a receiver has data-hiding key, he extracts additional data though he don't know the image content. If the receiver has encryption key, he can decrypt received data to obtain an image matches to the original one, but cannot extract additional data. If the receiver has both data-hiding key as well as encryption key, he can extract additional data and recover original content without any error by exploiting spatial correlation in the natural image when amount of additional data is more than 50 words.

Keywords: Image Processing, Encryption, IRIS Image, Cancelable Biometrics.

1. INTRODUCTION

Due to their effectiveness, usefulness, and dependability, biometric technologies are expanding and being used in a wide range of applications, including border control, authentication systems, and healthcare [1]. Because they solve the problems associated with managing passwords and tokens, biometric authentication systems are preferred over traditional authentication systems based on passwords and/or tokens. However, the widespread use of biometrics in authentication systems has given rise to various security and privacy problems [2]. This is important to note because biometrics cannot be canceled or reversed, as in contrast to tokens and passwords. Therefore, it is impossible to use the biometric characteristic in another application if the attacker is successful in compromising the biometric template in one. Additionally, users may be tracked by cross-matching biometric databases in those programs if the same biometric feature is used in many applications. In the past few years, several biometric template protection constructions have been presented to solve security and privacy concerns related to biometrics. Cancellable biometrics (CB) [3] and biometric cryptosystems [4] are two of the more well-known of these constructs. The primary objective of CB schemes is to identify several alternative distorted or unlinkable variations of a given user's biometric template to enroll the user in various applications that share that biometric attribute. For these techniques to be implemented in authentication systems, they must meet three requirements. The practical CB system must specifically meet the following conditions [5]:

https://www.doi.org/10.58257/IJPREMS31211

• Irreversibility. It should be computationally impossible to recover a biometric template that is sufficiently comparable to the original from one or more compromised cancelable templates. When given to the same authentication system, recovered biometric templates are considered sufficiently equal to the original template if they are accepted as having been created from a valid probing sample.

• Revocability. Revocability should allow for the replacement of a compromised cancelable template with a new, protected template. This replacement process shouldn't affect other protected templates that were created from the same original.

• Non-linkability. If two cancelable templates are descended from the same user, it cannot be assumed that they are non-linkable. By fulfilling the criteria, hackers and attackers are prevented from cross-matching multiple cancelable templates across different applications.

• Recognition accuracy preservation. The recognition accuracy of the underlying authentication system shouldn't be considerably impacted by cancellable transformation. The transformation process must not cause the matching accuracy to degrade.To satisfy the aforementioned requirements, various CB schemes often generate cancelable templates using a combination of a) biometric data b) application-specific c) user-specific helper data (e.g., random keys or passwords), which are typically kept on independent tokens [6] - [7]. Although employing distinct user-specific tokens in different applications may be able to satisfy the revocability criterion, irreversibility, and non-linkability criteria cannot be guaranteed with such user-specific tokens. This is because the fact that a more thorough security examination of CB schemes should presumptively assume that the adversary is aware of the transformation process and has access to both the cancelable template and the coadjutor data particular to stoners. This assumption is plausible because handling data specific to stoners would experience the same problems as the traditional word- and/or commemorative-based authentication approaches. That is, it is possible to guess the data and/or lose or steal the commemorative. To defend against implicit sequestration and security attacks under the stolen-token script, a workable CB scheme should be suitable. The trade-off between security and recognition-delicacy preservation requirements needs to be fully explored to close the gap between theory and practice. Although it is asserted that the majority of the suggested CB schemes are resistant to the well-known reversibility and linkability attacks, these assertions are based on illogical, heuristic, or impractical justifications. For instance, the creators of some CB schemes illustrate the security aspects of their designs under particular transformation parameter settings and exhibit their designs' dedication to the preservation of recognition delicacy under various parameter settings. The security of many CB methods against invertibility and linkability attacks is overstated or cannot be guaranteed without a major decrease in recognition delicacy, according to several recent studies (15–26). To determine the success of promoting similar schemes in actual operations, it is crucial to evaluate the security components of modern CB schemes. Recently, Zhao et al. (6) developed a novel original ranking-based CB technique for guarding iris canons, which is now known as LRCB. As a result of its reliability, sturdiness, and unification, iris biometrics are frequently utilized in authentication systems. In this method, double iris canons are transformed into cancelable templates that can exercise arbitrary strings that are particular to an operation and have a decimal value. It has been demonstrated in (6) that the LRCB may preserve the recognition delicacy of the underlying iris recognition system while protecting stoner sequestration for correctly selected values of the metamorphosis parameters. It has also been asserted (see claim 6 below) that LRCB satisfies the requirements of irreversibility, revocability, and non-linkability. Because the LRCB scheme is a relatively recent CB scheme, it is not as well-known as other schemes that were first presented several years ago, such as BioHashing (7) and Bloom sludge grounded methods. However, experimenters who would be interested in creating analogous schemes would base their work on flawed CB schemes if the security packages of new CB schemes, such as the LRCB, aren't fully analyzed and estimated as soon as they're introduced to the scientific community. Because of this, identifying security flaws and vulnerabilities in current CB schemes, like the LRCB scheme, can help to improve the security of these schemes by exploring potential fixes for the flaws, as was the case with BioHashing and Bloom sludge-based template protection schemes. This design looks into the practicality of LRCB in terms of both recognition delicacy and CB security conditions. By using the distribution of order statistics for various random factors, we demonstrate how the LRCB metamorphosis process can be reversed to recover the original iris data from the defended rank values.The LRCB's weaknesses concerning recording multifariousness and linkability attacks are also addressed using the proposed reversibility attack. In contrast to what is asserted in (6), our empirically verified theoretical results show that the security of LRCB is significantly overestimated because it cannot maintain recognition delicacy without jeopardizing the security criteria of the CB construct. The standard signal processing typically occurs before encryption or after decryption since encryption transforms the regular signal into ungraspable data, making it an efficient and common method for sequester protection. However, in some scripts, the option to change the translated data while keeping the plain text hidden is requested since the content owner does not trust the processing service provider. For instance, a channel provider without access to the cryptographic key may seek to compress the translated data due to the channel's restricted resources when transmitting secret data. A Standard source law is used to first compress the source to its entropy rate. Additionally, one of the several widely used encryption schemes is used to translate the compressed source. Decryption happens first at the receiver, then relaxing. There is a lot of research interest in data compression of translated data. To eliminate redundancy and transfer spare data securely and effectively, it is customary to first compress the data and then cipher it to obscure its meaning. To retrieve the original data, the decryption and relaxation processes are carefully carried out at the receiver side However, in some operation scripts, a sender must convey data to a receiver and wishes to maintain the confidentiality of the information by using a network driver to supply the channel resource. Accordingly, the sender should encrypt the source

data, and the network provider may tend to compress the translated data without being aware of the source data's original encryption key. To recreate the original data at the receiver side, a decoder integrating relaxation and decryption functions will be utilized.In the translated image, reversible data is explored. The majority of research on reversible data concealing focuses on embedding/rooting data in the simple spatial sphere. However, in some operations, a subpar assistant or channel director will attempt to tack on some new message, such as the image's provenance, a note about it, or authentication information, even when he is unaware of the content of the original image. After picture decryption and communication initiation at the receiver side, it is also hoped that the original content would be recovered error-free. The original image is encrypted by the content owner using an encryption key, and new data can be inserted into the translated image using a data-hiding critical even when the data-hider is unaware of the original content. A receiver can first decrypt a translated image containing new data using the encryption key, then extract the hidden data using the data-hiding key, and then retrieve the original image using the encryption key. The scheme prevents the content decryption from being divided from the data genesis. And if someone possesses the data-caching key but not the encryption key, he will be unable to extract any information from the translated image containing new data. In other words, the fresh data must be plucked from the deciphered image for the star content of the original image to be exposed before data birth.

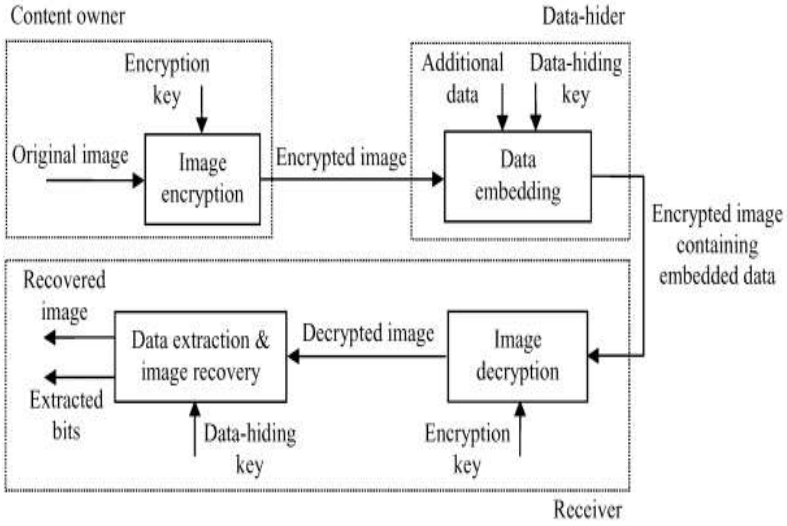

Figure 1.1 Reversible Data Hiding

The remainder of this essay is structured as follows:

Section 2 describes earlier works and their shortcomings while reviewing the current security measures under recent studies. The study's proposed approach is presented in Section 3. Findings are presented in Section 4, and the study is concluded in Section 5.

2. LITERATURE REVIEW

The authors of this research (5) claimed that a vital condition for the widespread adoption of biometric technology is demonstrating the security of cancelable biometrics and other template protection methods. A cancelable biometrics approach called BioEncoding has recently been put forth to encompass biometric templates encoded as double strings, such as iris canons. BioEncoding doesn't include any commemorative items or keys that are exclusive to stoners, unlike other template protection systems. Additionally, it complies with the requirements of undetectable biometrics without sacrificing the appropriate delicacy. However, before proposing BioEncoding for widespread use, its security against intelligent assaults such as correlation and optimization-grounded attacks must be demonstrated. The security of BioEncoding is examined in this study in terms of both sequestration protection and non-invertibility. The first step is to precisely define the resilience of defensive templates created using BioEncoding against brute-force hunt attacks. Also referenced and explained are BioEncoding's vulnerabilities to optimization grounded attacks and correlation attacks. To improve the BioEncoding algorithm's security against correlation attacks, a significant change is also suggested. Using the CASIA-IrisV3-Interval dataset, it is empirically explored how introducing this correction into BioEncoding affects the matching delicacy. Experimental findings support the proposed revision's effectiveness and demonstrate that it has no detrimental effects on the matched delicacy. Despite having many usability advantages over conventional authentication systems, biometrics-based authentication solutions have several security and sequestration issues (8). As a result, several template protection strategies have been put out in recent years to address these problems (9). In general, there are two primary categories of template protection methods: cancelable biometrics (CB) and

videlicet, biometric encryption (BE). In BE techniques, such as fuzzy commitment (10), fuzzy extractors (11), and fuzzy vaults (12), stoner-specific keys are linked with biometric templates to create a biometrically translated pseudo-identity for the stoner. This ensures that the key can only be released if the true biometric template is present during verification. However, CB styles, which are comparable to distorting transforms (13), BioHashing (14), and BioEncoding (15), create revocable defended templates from true biometric templates by applying various non-invertible transforms to those true templates in various processes. After applying the same transfigure (applied in registration) to a new template during authentication, matching is carried out in the transfigure sphere. All template protection schemes must satisfy the ensuing conditions

Delicacy:

The performance of the vulnerable biometric system's recognition shouldn't significantly decline as a result of a template protection technique.

Revocability:

If a protected template is taken or compromised, it should be simple to drop (cancel) it.

Irreversibility:

It should be computationally impossible to recover the original templates from protected bones.

Diversity:

For the same biometric, it should be possible to generate a huge number of defended templates (to be used in various procedures).

Unlinkability:

An opponent shouldn't be able to ascertain which defended templates are used by the same user.

Although demonstrating the delicacy and revocability conditions in nearly all template protection styles proposed in the literature so far has received significant attention, assuring the security of related systems strictly has received less attention. Numerous experimenters have recently explored the security shortcomings of a few template protection techniques. They concluded that the irreversibility and diversity of a recently suggested cancelable biometrics scheme, BioEncoding, were analyzed for its security features. Attacks were conducted in three different orders: brute-force hunt, correlation, and optimization-based. It has been established that BioEncoding is susceptible to correlation attacks despite being resistant to brute-force and optimization-based attacks. They put out three distinct strategies to strengthen BioEncoding's defenses against correlation attacks. Experimental results supported our study and demonstrated the efficacy of the suggested modifications to BioEncoding in terms of security and delicacy using the CASIA-V3-Interval dataset. In this paper (2) the authors stated that cancelable biometric schemes induce secure biometric templates by combining stoner-specific commemoratives and biometric data. The primary goal is to create irreversible, irrevocable templates with great comparative sensitivity. In this paper, they cryptanalyse two recent cancelable biometric schemes grounded on a particular position-sensitive mincing function, indicator-of-maximum (IoM) Gaussian Random Projection-IoM (GRP-IoM) and Slightly Random Permutation-IoM (URP-IoM). As first proposed, these schemes were claimed to be resistant to reversibility, authentication, and linkability attacks under the stolen token script. They proposed several attacks against GRP-IoM and URP-IoM, and argue that both schemes are oppressively vulnerable to authentication and linkability attacks. They also proposed better, but not yet practical, reversibility attacks against GRP-IoM. The correctness and practical impact of our attacks are vindicated over the same dataset handed by the authors of these two schemes. Biometrics has been extensively espoused in authentication systems, border control mechanisms, fiscal services, and healthcare operations. Biometric technologies are veritably promising to give stoner-friendly, effective, and secure results to practical problems. In a typical bio-metric grounded authentication scheme, druggies register their biometric-affiliated information with the system, and they are authenticated grounded on a similarity score calculated from their enrolled biometric data and the fresh biometric they give. As a consequence, service providers need to manage biometric databases. This is kindly similar to storing and managing stoner watchwords in a word-grounded authentication scheme. The main difference is that biometric data serves as a long-term and unique particular identifier, whence distributed as largely sensitive and private data. This isn't the case for watchwords as they can be chosen independent of any stoner-specific characteristics, a single stoner can produce an independent word per operation, and watchwords can be abandoned, changed, and renewed fluently at any time. As a result, managing biometric data in operations is more grueling, and it requires further care. As biometric-grounded technologies are stationed at a larger scale, biometric databases come natural targets in cyber attacks. To alleviate security and sequestration problems in the use of biometrics, several biometric template protection styles have been proposed, including cancelable biometrics, biometric cryptosystems (e.g. fuzzy extractors), keyed biometrics (e.g. homomorphic encryption), and mongrel biometrics. In this paper, they concentrated on cancelable biometrics (CB). In CB, a biometric template is reckoned through a process where the main inputs are biometric data (e.g. biometric image, or the uprooted

point vector) of a stoner, and a stoner-specific commemorative (e.g. arbitrary key, seed, or a word). In a nutshell, templates can be abandoned, changed, and renewed by changing stoner-specific commemoratives. For the security of the system, the template generation process should be non-invertible (unrecoverable) given the biometric template and/ or the commemoration of a stoner, it should be computationally infeasible to recover any information about the underpinning biometric data. Also, given a brace of biometric templates and the corresponding commemoratives, it should be computationally infeasible to distinguish whether the templates were deduced from the same user (unlinkability). They should note that indeed though stoner-specific commemoratives in CB are perhaps considered as secret, as part of a two-factor authentication scheme, cryptanalysis of CB with stronger inimical models generally assume that the bushwhacker knows both the biometric template and the commemorative of a stoner. This is a presumptive supposition in practice because a stoner commemorative may have low entropy (e.g. a weak word), or it may just be compromised by a bushwhacker. This script is also known as the stolen-token script. They concluded that they homogenized the authentication, irreversibility, and unlikability sundries under the stolen token script, and proposed several attacks against GRP-IoM and URP-IoM. We argued that both schemes are oppressively vulnerable to authentication and linkability attacks. Grounded on their experimental results, they estimated100success rate for their authentication attacks against GRP-IoM and URP-IoM, 97 success rate for our linkability attacks against GRP-IoM, and 83success rate for their linkability attacks against URP-IoM. They also proposed better reversibility attacks against GRP-IoM, but they aren't practical yet. They believed that their attacks can further be bettered. One intriguing exploration direction would be to see the impact of different choices of objective functions in modeling the optimization problems in the authentication and reversibility attacks. Also, it would be intriguing to exploit different correlation criteria in linkability attacks. Eventually, they assumed that adversaries aren't adaptive and they aren't allowed to ask queries for data of their choices in our attack models. This is rather a weak inimical model. Thus, they anticipated that their attacks can further be bettered by allowing stronger adversaries. In this paper (3) the authors stated that biometric recognition is an integral element of ultramodern identity operation and access control systems. Due to the strong and endless link between individualities and their biometric traits, exposure of enrolled druggie‘s biometric information to adversaries can seriously compromise biometric system security and stoner sequestration. Multitudinous ways have been proposed for biometric template protection over the last 20 times. While these ways are theoretically sound, they infrequently guarantee the asked non-invertibility, revocability, and non-linkability parcels without significantly demeaning the recognition performance. The idea of this work is to dissect the factors contributing to this performance gap and highlight promising exploration directions to ground this gap. The design of steady biometric representations remains an abecedarian problem, despite recent attempts to address this issue through point adaption schemes. The difficulty in estimating the statistical distribution of biometric features not only hinders the development of better template protection algorithms but also diminishes the capability to quantify the non-invertibility and non-linkability of algorithms. Eventually, achieving non-linkability without the use of external secrets (e.g., watchwords) continues to be a grueling proposition. Further exploration of the below issues is needed to cross the ocean between proposition and practice in biometric template protection.

BIOMETRIC-

recognition, or biometrics, refers to the automated recognition of individualities grounded on their biological and behavioral characteristics (e.g., face, point, iris, win/ cutlet tone, and voice). While biometrics is the only dependable result in some operations (e.g. border control, forensics, covert surveillance, and identify-duplication), it competes with or complements traditional authentication mechanisms similar to watchwords and commemoratives in operations-quiring verification of a claimed identity (e.g., access control, fiscal deals, etc.,). Though factors similar to fresh cost and vulnerability to caricature attacks hamper the proliferation of biometric systems in authentication operations, security and sequestration enterprises related to the storehouse of biometric templates have been major obstacles. A template is a compact representation of the tasted bio-metric particularity containing salient discriminative information that's essential for feting the person (see Figure 1). Exposure of biometric templates of enrolled druggies to adversaries can affect the security of biometric systems by enabling the donation of spoofed samples and renewal attacks. This trouble is compounded by the fact that biometric traits are irreplaceable. Unlike watchwords, it isn't possible to discard the exposed template and re-up the stoner grounded on the same particularity. Also, it's possible to stealthily cross-match templates from different databases and descry whether the same person is enrolled across different unconnected operations. This can oppressively compromise the sequestration of individuals enrolled in biometric systems. In utmost functional (stationed) biometric systems, the biometric template is secured by cracking it using standard encryption ways similar to Advanced Encryption Standard (AES) and RSA cryptosystem. This approach has two main downsides. Originally, the translated template will be secure only as long as the decryption key is unknown to the bushwhacker. Therefore, this approach simply shifts the problem from biometric template protection to cryptographic crucial operation, which is inversely grueling. In this paper (4) the authors stated that Human authentication is the security task

whose job is to limit access to physical locales or computer networks only to those with authorization. This is done by equipping authorized druggies with watchwords commemoratives or using their biometrics. Unfortunately, the first two suffer a lack of security as they're easily forgotten and stolen; indeed biometrics also suffers from some essential limitations and specific security pitfalls. A more practical approach is to combine two or further factor authenticators to reap benefits in security or accessibility or both. This paper proposed a new two factors authenticator grounded on dinned inner products between tokenized pseudo-random number and the stoner-specific point, which is generated from the integrated sea and Fourier – Mellin transfigure, and hence produces a set of stoner-specific compact law that chased as BioHashing. BioHashing is largely tolerant of data prisoner equipoises, with the same stoner point data performing in largely identified bitstrings. Also, there's no deterministic way to get the stoner-specific law without having both commemorative with arbitrary data and a stoner point. This would cover us for the case against biometric fabrication by changing the stoner-specific credential, which is as simple as changing the commemorative containing the arbitrary data. BioHashing has significant functional advantages over sole biometrics i.e., zero equal error rate point and clean separation of the genuine and pretender populations, thereby allowing the elimination of false accept rates without suffering from the increased circumstance of false reject rates. In this paper (5) the authors stated that Biometric recognition is more and more employed in authentication and access control of colorful operations. Biometric data are explosively linked with the stoner and don't allow revocability or diversity, without acclimated post-processing. Cancelable biometrics, including the veritably popular algorithm BioHashing, is used to manage the underpinning sequestration and security issues. The principle is to transfigure a biometric template in a BioCode, to enhance stoner sequestration and operation security. These schemes are used for template protection of several biometric modalities, such as Bioprints or face, and the robustness is generally related to the hardness to recover the original biometric template by fraud. In this paper, they proposed to use inheritable algorithms to compare the original biometric point and caricature the authentication system. They showed through experimental results on Bioprints the effectiveness of the proposed attack on the BioHashing algorithm, by approximating the original BioCode, given the seed and the corresponding BioCode.

3. PROPOSED METHODOLOGY

The existing scheme is made up of image encryption, with data embedding and data extraction-based image-recovery phases. The content creator encrypts the original uncompressed image using a given encryption key to yield a translated image. Also, the data-hider compresses the Least Significant Bits (LSB) of the translated images using the data-caching key to produce a meager space to accommodate the new data. At the receiver side, data embedded in the created space is fluently recaptured from the translated image containing fresh data according to the data-hiding key. Since data embedding only affects LSB, the decryption with the given encryption key can affect the image analogous to the original interpretation. When using both encryption and data-hiding keys, the embedded fresh data is successfully uprooted and the original image can be impeccably recovered by exploiting the spatial correlation in the natural image.

• Separate garbling mechanisms are used for image encryption and data caching.

• Operates on Argentine scale image data only.

• Carrier image must be large since one bit per pixel is used.

The proposed system implements all the being system methodologies. In addition, the RGB color image is taken for image encryption. During image encryption, pseudo-random bits are X-or with image pixel bits as in being system.

During the reverse process, either the original image or textbook alone can be recaptured by the receiver. In addition, textbook input data is perturbed similar to that arbitrary characters are bed inside the original textbook. Also, the textbook data is translated using Triple DES encryption and also hidden in the translated image.

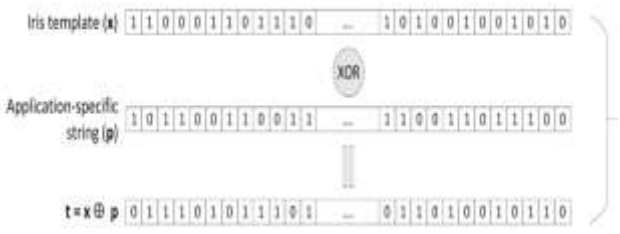

Figure 3.1 Transformation of Iris Template

4. FINDINGS

- The same encoding mechanisms can be used for image encryption and data hiding.
- Operates on RGB image data also.
- The two least significant bits of the given pixel can also be used for data hiding.

- Small carrier image also supports more data hiding than the existing system.
- Text perturbation and Triple DES encryption make the application more secure.

5. CONCLUSION

This project implements the scheme of separable reversible data hiding in iris images using the RGB-LSB method. Inseparable reversible data hiding at the receiver side when the receiver has a data-hiding key only he can extract the confidential data and to recover the original content and extract the additional data the receiver must have both the keys encryption key as well as data-hiding key. By using the novel RGB-LSB method for embedding the data, the size of the net payload can be increased sufficiently. That is we can hide enough data into the encrypted image and also examine the performance of the existing method and proposed method images in terms of parameters like signal-to-noise ratio values, size of the cover image, data capacity, etc. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

6. REFERENCES

[1] O. Ouda, N. Tsumura, and T. Nakaguchi, ‘‘On the security of BioEncodingbased cancelable biometrics,’’ IEICE Trans. Inf. Syst., vol. E94.D, no. 9, pp. 1768–1777, 2011.

[2] Ghammam, K. Karabina, P. Lacharme, and K. Thiry-Atighehchi,‘‘ A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2869–2880,2020.

[3] K. Nandakumar and A. K. Jain, ‘‘Biometric template protection: Bridging the performance gap between theory and practice,’’ IEEE Signal Process.Mag., vol. 32, no. 5, pp. 88–100, Sep. 2015.

[4] A. T. B. Jin, D. N. C. Ling, and A. Goh, ‘‘BioHashing: Two-factor authentication featuring fingerprint data and tokenized random number,’’ Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

[5] P. Lacharme, E. Cherrier, and C. Rosenberger, ‘‘Preimage attack on Bio-Hashing,’’ inProc. Int. Conf. Secure. Cryptogr. (SECRYPT), 2013, pp. 1–8

[6] D. Zhao, S. Fang, J. Xiang, J. Tian, and S. Xiong, ‘‘Iris template protection based on local ranking,’’ Secur. Commun. Netw., vol. 2018, pp. 1–9, Jan. 2018.

[7] A. T. B. Jin, D. N. C. Ling, and A. Goh, ‘‘BioHashing: Two-factor authentication featuring fingerprint data and tokenized random number,’’ Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, Nov. 2004.

[8] S. Prabhakar, S. Pankanti, and A.K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Secur. Privacy Mag., vol.1, no.2, pp.33–42, March 2003.

[9] [9] A.K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP J. Adv. Signal Process., p.579416, 2008.

[10] A. Juels and M.A. Wattenberg, “A fuzzy commitment scheme, ”Proc. 6th ACM Conf. Computer & Communications Security, pp. 28–36, 1999.

[11] F. Hao, R. Anderson, and J. Daugman, “Combining crypto with bio-metrics effectively,” IEEE Trans. Comput., vol.55, no.9, pp.1081–1088, Sept. 2006.

[12] A. Jules and M. Sudan, “A fuzzy vault scheme,” Proc. IEEE Int.Symp. Info. Theory, p.408, 2002.[6] N.K. Ratha, S. Chikkerur, J.H. Connell, and R. Bolle, “Generating cancelable fingerprint templates,” IEEE Trans. Pattern Anal. Mach.Intell., vol.29, no.4, pp.561–572, April 2007.

[13] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, “BioHashing: Two-factor authentication featuring fingerprint data and tokenized random number,” Pattern Recognit., vol.37, no.11, pp.2245–2255, Nov. 2004.