Secured Information Transmission Using Biometric System

T.Saravanan[1], P.Abinaya[2], C.Bharathi[3], S.Deepika[4], B.Ramyadevi[5]
[1]Assistant Professor ,Dept of information technology
[2, 3, 4, 5]Dept of information technology
[1, 2, 3, 4, 5] Vivekanandha College of Engineering for Women (Autonomous),
Tiruchengode, Namakkal-637205, Tamil Nadu, India.

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.

I. INTRODUCTION

Biometric technologies are being increasedand used in the wide variety of applications like health care, authentication systems, and border control, due to their efficiency, usability, and reliability [1]. Biometrics-based login/authentication systems are preferred among conventional authentication systems based upon passwords and/or tokens as they are alleviating password/token management issues. But, several security and also privacy concerns have been raised as result of wide-spread biometrics deployment in authentication systems [2].

This is mainly because, unlike token, passwords, biometrics cannot be canceled or revoked. Hence, if the attacker manages to compromise the biometric template in one application, it is not possible to use the biometric characteristic in another application. In addition, if same biometric characteristic is employed in the several applications, users may be tracked by cross-matching biometric databases in those applications.

To address security as well as privacy issues inherent in biometrics, several biometric templates protection constructs are being proposed in past few years. Out of these construct, cancelable biometrics [CB] [3] and biometric cryptosystems [4] are popular among them. The CB schemes‘main goal is to find multiple different distorted / non-linkable versions of same biometric template of given user so that to be enrolled in various applications with same biometric trait. These schemes will satisfy three conditions in order to deployinauthentication systems practically. Specifically, the practical CB scheme msut satisfy the requirements below [5]:

- Irreversibility. Irreversibility should be computationally infeasible to recover the sufficiently similar version of original biometric template from single or multiple compromised cancelable templates. Recovered biometric templatesare sufficiently equal to original template if it is recognized as if it was prepared from a legitimate probe sample when presented to same authentication system.

- Revocability. Revocability should be possible to revoke a compromised cancelable template, re-issue a new protected template to replace that template. Other protected templates which are generated from same original should not be affected by this replacement process.
- Non-linkability. Non-linkability must not be possible to guessif two cancelable templates are derived from same user.Satisfying the requirement disallowshackers/attackersfromperforming cross-matching among multiplecancelable templates across various applications.
- Recognition accuracy preservation. Cancelable transformation should not affect recognition accuracy of theunderlyingauthenticationsystemsignificantly. The matching accuracy must not deteriorate as the result of transformation process.

Typically, these CB schemes are generating cancelable templates using combineda) biometric data b) application-specific and/or c) user-specific helper data (e.g., random keys or passwords), usually stored on independent tokens, to fulfill above-mentioned requirements [6] – [7]. But, although revocability requirement might be fulfilled by using the different user-specific tokens in various applications, satisfyingirreversibility and non-linkability requirements could not be guaranteed relying on such user-specific tokens.

This is because a further rigorous security analysis of CB schemes should assume that the adversary is familiar with metamorphosis process and knows both the cancelable template and stoner-specific coadjutor data. This supposition is reasonable because the process of managing the stoner-specific data would suffer from the same issues essential to conventional word and/ or commemorative- grounded authentication styles. That is, the data can be guessed and/ or the commemorative can be lost or stolen.

Thus, a practical CB scheme should be suitable to repel implicit sequestration and security attacks under the stolen-token script. In order to bridge the gap between proposition and practice, the trade-off between security and recognition- delicacy preservation conditions should be completely delved.

Although it's claimed that utmost of the proposed CB schemes are secure against well- known reversibility and linkability attacks, these claims are grounded on intuitive, heuristic, or impracticable arguments. For case, the authors of some CB schemes demonstrate the security parcels of their styles under specific metamorphosis parameter settings and show the commitment of their styles to the recognition delicacy preservation under different parameter settings.

Several recent studies (15) – (26) showed that the security of numerous CB schemes against invertibility and linkability attacks are overrated or can not be assured without significant deterioration in recognition delicacy. Thus, assaying the security parcels of recent CB schemes is of consummate significance in order to assess the felicity of espousing similar schemes in practical operations.

Lately, Zhao etal. (6) proposed a new original ranking- grounded CB scheme, henceforth called LRCB, for guarding iris- canons. Iris biometrics is generally used in authentication systems due to its trustability, stability, and oneness.

In this scheme, double iris- canons are converted into decimal- valued cancelable templates exercising operation-specific arbitrary strings. It has been shown in (6) that, for suitably chosen values of the metamorphosis parameters, LRCB can save the recognition delicacy of the underpinning iris recognition system while guarding stoner sequestration.(6) has also been claimed) that LRCB satisfies the irreversibility, revocability andnon-linkability conditions.

The LRCB scheme is a fairly new CB scheme and therefore it isn't a veritably well- known scheme compared to other schemes that were firstly proposed several times ago similar as BioHashing (7) and Bloom sludge- grounded schemes.

Still, if the security parcels of new CB schemes, similar as the LRCB, aren't completely anatomized and estimated as soon as they're introduced to the scientific community, experimenters who might be interested in developing analogous schemes would predicate their work on defective CB schemes.

Therefore, discovering security excrescencies and vulnerabilities in recent CB schemes, similar as the LRCB scheme, can play an important part in perfecting the security of these schemes by chancing suitable remedies for the discovered blights as in the case for BioHashing and Bloom sludge- grounded template protection schemes.

This design investigates the practicality of LRCB in terms of the CB security conditions as well as recognition delicacy. We show that the metamorphosis process of LRCB can be reversed employing the distribution of order-statistics for separate arbitrary variables in order to recover the original iris-data from the defended rank values.

Also, they use the proposed reversibility attack to readdress the vulnerabilities of LRCB with respect to record multifariousness and linkability attacks. Our empirically validated theoretical results demonstrate that, in discrepancy to what's claimed in (6), the security of LRCB is largely overrated since it can not retain recognition delicacy without immolating the security conditions of the CB construct.

As an effective and popular means for sequestration protection, encryption converts the ordinary signal into ungraspable data, so that the traditional signal processing generally takes place before encryption or after decryption.

Still, in some scripts that a content proprietor does not trust the processing service provider, the capability to manipulate the translated data when keeping the plain content undisclosed is asked. For case, when the secret data to be transmitted are translated, a channel provider without any knowledge of the cryptographic key may tend to compress the translated data due to the limited channel resource.

The source is first compressed to its entropy rate using a standard source law. Also, the compressed source is translated using one of the numerous extensively available encryption technologies. At the receiver, decryption is performed first, followed by relaxation. Compression of translated data has attracted considerable exploration interest. The traditional way of securely and efficiently transmitting spare data is to first compress the data to reduce the redundancy, and also to cipher the compressed data to mask its meaning. At the receiver side, the decryption and relaxation operations are orderly performed to recover the original data.

Still, in some operation scripts, a sender needs to transmit some data to a receiver and hopes to keep the information nonpublic to a network driver in provides the channel resource for the transmission.

That means the sender should cipher the original data and the network provider may tend to compress the translated data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating relaxation and decryption functions will be used to reconstruct the original data.

The reversible data hiding in translated image is delved. Utmost of the work on reversible data hiding focuses on the data embedding/ rooting on the plain spatial sphere. But, in some operations, an inferior adjunct or a channel director hopes to tack some fresh communication, similar as the origin information, image memorandum or authentication data, within the translated image though he doesn't know the original image content.

And it's also hopeful that the original content should be recovered without any error after image decryption and communication birth at receiver side.
A content proprietor encrypts the original image using an encryption key, and a data-hider can bed fresh data into the translated image using a data-hiding crucial though he doesn't know the original content.

With an translated image containing fresh data, a receiver may first decipher it according to the encryption key, and also prize the bedded data and recover the original image according to the data-hiding key. In the scheme, the data birth isn't divisible from the content decryption.
In other words, the fresh data must be uprooted from the deciphered image, so that the star content of original image is revealed before data birth, and, if someone has the data-caching key but not the encryption key, he can not prize any information from the translated image containing fresh data.

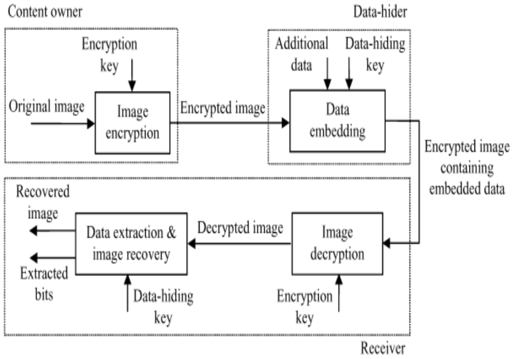

Figure 1.1 Reversible Data Hiding

The rest of this paper is organized as follows: Section 2 reviews the existing security approaches under recent studies andexplainsprevious works and their drawbacks. Section 3 provides proposed methodology of the study.Section 4 provides finds and Section 5 is conclusion of the study.

II. LITERATURE REVIEW

In this paper (5) the authors stated that proving the security of cancelable biometrics and other template protection ways is a crucial prerequisite for the wide deployment of biometric technologies. BioEncoding is a cancelable biometrics scheme that has been proposed lately to cover biometric templates represented as double strings like iris canons. Unlike other template protection schemes, BioEncoding doesn't bear stoner-specific keys or commemoratives.

Also, it satisfies the conditions of untraceable biometrics without immolating the matching delicacy. Still, the security of BioEncoding against smart attacks, similar as correlation and optimization- grounded attacks, has to be proved before recommending it for practical deployment. In this paper, the security of BioEncopding, in terms of bothnon-invertibility and sequestration protection, is anatomized. First, resistance of defended templates generated using BioEncoding against brute- force hunt attacks is redefined strictly. Also, vulnerabilities of BioEncoding with respect to correlation attacks and optimization grounded attacks are linked and explained.

Likewise, an important revision to the BioEncoding algorithm is proposed to enhance its security against correlation attacks. The effect of integrating this revision into BioEncoding is validated and its impact on the matching delicacy is delved empirically using CASIA-IrisV3-Interval dataset. Experimental results confirm the efficacity of the proposed revision and show that it has no negative impact on the matching delicacy.

Although biometrics- grounded authentication systems parade numerous usability advantages over traditional authentication systems, they suffer from several security and sequestration enterprises (8). As a result, numerous template protection techniqueshave been proposed in the last many times to deal with these issues (9). Generally, template protection ways may beclassified into two main orders; videlicet, biometric encryption (BE) and cancelable biometrics (CB).

In BE tech-niques, similar as fuzzy commitment (10), fuzzy extractors (11), and fuzzy vaults (12), biometric templates are linked witha stoner-specific key to produce a biometrically translatedpseudo-identity for the stoner so that the key can be released only if the true biometric template is present on verifica-tion. On the other hand, CB styles, similar as distorting transforms (13), BioHashing (14), and BioEncoding (15), induce revocable defended templates from true biometric templates through applying differentnon-invertible transforms to true templates in different operations.

Matching is done in the transfigure sphere after applying the same transfigure (applied in registration) to a fresh template during authentication. Any template protection scheme should satisfy the ensuing conditions

Delicacy: A template protection scheme shouldn't intro-duce significant declination in the recognition performance of the vulnerable biometric system.

Revocability: It should be easy to drop (cancel) a defended template if it's stolen or compromised.

Irreversibility: Reacquiring original templates from defended bones should be computationally infeasible.

Diversity: It should be possible to induce large number of defended templates (to be used in different operations) for the same biometric.

Unlinkability: It shouldn't be possible for an adversary to determine whether different defended templates belong to the same user.

Although importantattention has beengiven to proving the delicacy and revocability conditions in nearly all template protectionstylesproposed in the literature so far, lowerattention has beenpaid to assaying the security of similarsystemsstrictly. Justlately, a manyexperimentershavestudied the securityexcrescencies of some template protectionschemes.

They concluded that, the securityaspects of a latelyproposed cancelable biometrics scheme, BioEncoding, were anatomized with respect to irreversibility and diversity. Three differentorders of attacks were delvedbrute-forcehuntattacks, correlation attacks and optimization-groundedattacks.

It has beenshown that although BioEncoding is secure against brute- forceattacks and optimization-groundedattacks, it's vulnerable to correlation attacks. They proposed three differentapproaches to enhance the security of BioEncoding against correlation attacks. Experimentalresults usingCASIA-V3-Interval dataset validated our analysis and con- concrete the effectiveness of the proposedvariations to BioEncoding in terms of security and delicacy.

In this paper (2) the authorsstated that cancelable biometric schemesinducesecure biometric templates by combiningstonerspecificcommemoratives and biometric data. The main ideal is to produceunrecoverable, unlinkable, and revocable templates, with highdelicacy of comparison.

In this paper, they cryptanalyze two recent cancelable biometric schemesgrounded on a particularpositionsensitivemincingfunction, indicator-of-maximum (IoM) Gaussian Random Projection-IoM (GRP-

IoM) and Slightly Random Permutation-IoM (URP-IoM). As firstlyproposed, these schemes were claimed to be resistant against reversibility, authentication, and linkability attacks under the stolen token script. The proposed several attacks against GRP-IoM and URP-IoM, and argue that both schemes are oppressivelyvulnerable against authentication and linkability attacks.

They alsoproposed better, but not yetpractical, reversibility attacks against GRP-IoM. The correctness and practicalimpact of our attacks are vindicated over the same dataset handed by the authors of these two schemes.

Biometrics has beenextensivelyespoused in authentication systems, bordercontrol mechanisms, fiscalservices, and healthcare operations. Biometric technologies are veritablypromising to givestoner-friendly, effective, and secureresults to practicalproblems. In a typicalbio-metric grounded authentication scheme, druggiesregister their biometric-affiliatedinformation with the system, and theyare authenticatedgrounded on a similarityscorecalculated from their enrolled biometric data and the fresh biometric they give.

As a consequence, service providers need to manage biometric databases. This is kindlysimilar to storing and managingstonerwatchwords ina word- grounded authentication scheme.

The main difference is that biometric data serves as a long- term and uniqueparticular identifier, whence distributed as a largelysensitive and private data. This isn't the case for watchwords as they can bechosenindependent of any stonerspecific characteristics, a singlestoner can produce an independentword per operation, and watchwords can beabandoned, changed, and renewedfluently at any time. As a result, managing biometric data in operations is moregrueling, and it requires furthercare. As biometric- grounded technologies are stationed at a larger scale, biometric databases comenaturaltargets in cyber attacks.

In order to alleviatesecurity and sequestrationproblems in the use of biometrics, several biometric template protectionstyleshavebeenproposed, 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 uprootedpoint vector) of a stoner, and a stonerspecificcommemorative (e.g. a arbitrarykey, seed, or a word).

In a nutshell, templates can beabandoned, changed, and renewed by changingstonerspecificcommemoratives. For the security of the system, it's important that the template generationprocess isnon-invertible (unrecoverable) given the biometric template and/ or the commemorative 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 correspondingcommemoratives, it should be computationally infeasibleto distinguish whether the templates were deduced from the same user (unlinkability).

They should note that indeed though stoner specific commemoratives in CB 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 an 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 against 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, and83success 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 modelling the optimization problems in the authentication and reversibility attacks.

Also, it would be intriguing to exploit different correlation criteria in the 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 druggies'biometric information to adversaries can seriously compromise biometric system security and stoner sequestration. Multitudinous ways have been proposed for biometric template protection over the last20 times.

While these ways are theoretically sound, they infrequently guarantee the askednon-invertibility, revocability, andnon-linkability parcels without significantly demeaning the recognition performance. The ideal of this work is to dissect the factors contributing to this performance gap and high-light promising exploration directions to ground this gap. Design of steady biometric representations remains a 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 thenon-invertibility andnon-linkability of being algorithms. Eventually, achievingnon-linkability without the use of external secrets (e.g., watchwords) continues to be a grueling proposition. Farther exploration on 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 theirbio-logical 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 identityde-duplication), it competes with or complements traditional authentication mechanisms similar as watchwords and commemoratives in operationsre-quiring verification of a claimed identity (e.g., access control, fiscal deals,etc.).

Though factors similar as 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 tastedbio-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 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 stealthilycross-match templates from different databases and descry whether the same person is enrolled across different unconnected operations. This can oppressively compromise the sequestration of individualities enrolled in biometric systems.

In utmost functional (stationed) biometric systems, thebio-metric template is secured by cracking it using standard encryption ways similar as 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 network only to those with authorization. This is done by equipped authorized druggies with watchwords, commemoratives or using their biometrics.

Unfortunately, the first two suffer a lack of security as they're easy being forgotten and stolen; indeed biometrics also suffers from some essential limitation and specific security pitfalls. A more practical approach is to combine two or further factor authenticator to reap benefits in security or accessible or both.

This paper proposed a new two factor authenticator grounded on dinned inner products between tokenizedpseudo-random number and the stoner specific point point, which generated from the integrated sea and Fourier – Mellin transfigure, and hence produce a set of stoner specific compact law that chased as BioHashing. BioHashing largely tolerant of data prisoner equipoises, with 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 stoner point point. This would cover us for case against biometric fabrication by changing the stoner specific credential, is as simple as changing the commemorative containing the arbitrary data. The BioHashing has significant functional advantages over solely biometrics i.e., zero equal error rate point and clean separation of the genuine and pretender populations, thereby allowing elimination of false accept rates without suffering from 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 nor diversity, without an acclimatedpost-processing. Cancelable biometrics, including the veritably popular algorithm BioHashing, is used to manage with the underpinning sequestration and security issues.

The principle is to transfigure a biometric template in a BioCode, in order to enhance stoner sequestration and operation security. These schemes are used for template protection of several biometric modalities, as Bioprints or face and the robustness is generally related to the hardness to recover the original biometric template by an 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, byapproximating the original BioCode, given the seed and the corresponding BioCode.

III. 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 an translated image.

Also, the data-hider compresses Least Significant Bits (LSB) of translated image 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 in the image analogous to original interpretation. When using both of 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 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 encryptionpseudo-random bits areX-or with image pixel bits as in being system.

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

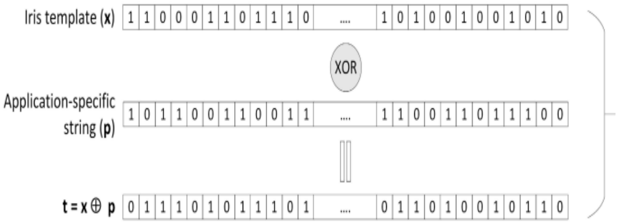

Figure 3.1 Transformation of Iris Template

IV. FINDINGS

- Same encoding mechanisms can be used for image encryption and data hiding.
- Operates on RGB image data also.
- Two least significant bits of a given pixels 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 makes the application more secure.

V. CONCLUSION

This project implements the scheme of separable reversible data hiding in iris images using RGB-LSB method. In separable reversible data hiding at the receiver side when the receiver has data-hiding key only he can extract the confidential data and to recover the original content and extract the additional data the receiver must has both of the keys encryption key as well as data-hiding key. Also 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 the enough data into the encrypted image and also examined the performance of 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.

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: Bridgingthe 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 factorauthentication featuring fingerprint data and tokenised 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. Secur. 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 tokenised 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] 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 num-ber,” Pattern Recognit., vol.37, no.11, pp.2245–2255, Nov. 2004.

[14] O. Ouda, N. Tsumura, and T. Nakaguchi, “BioEncoding: A reliabletokenless cancelable biometrics scheme for protecting IrisCodes,”IEICE Trans. Inf. & Syst., vol.E93-D, no.7, pp.1878–1888, July2010.

[15] A. Cavoukian and A. Stoianov, “Biometric encryption: The new breed of untraceable biometrics,” in Biometrics: Fundamentals, Theory, and Systems, ed. N.V. Boulgouris, K.N. Plataniotis, and E.Micheli-Tzanakou, Wiley-IEEE Press, 2009.