Contemporary Approaches On Reversible Data Hiding In Iris Image Using Deep Learning Techniques

M. Mary Shanthi Rani [1], S. Selvarani [2]

drmaryshanthi@gmail.com[1], rani.s.selva@gmail.com[2]

Research Supervisor, Associate Professor, Department of Computer Science & Applications, The Gandhigram Rural Institute (Deemed To Be University), Dindigul [1], Assistant Professor, Department Of Computer Applications, Fatima College, Mary Land, Madurai

Abstract. The concept of reversible data concealing is crucial for secret communication. After the extraction stages, the protected information can be completely rebuilt in addition to the hidden data being removed. Pixel, Block and Interpolation based algorithms have seen substantial development over the past decade, employing the spatial-frequency domain and other related techniques. The goal of this research work is to categorize and describe the various methods, inner groups and research papers related to the idea of Reversible Data Hiding (RDH). In order to protect privacy, this research suggests a revolutionary iris image data concealing strategy. Here, private information is incorporated into the iris image in a way that has the least negative effect on iris recognition. The Syndrome Trellis Coding (STC) architecture is applied, limiting changes to the embedded data and to the regions that infrequently affect iris identification. A new distortion function is also proposed to enumerate the impression of data implanting on recognition of Iris, which assigns high embedding cost to locations with strong iris features. According to experimental findings, enough information can be incorporated into the iris image while sustaining excellent identification accuracy by employing the proposed technique.

Keywords: Data hiding, Reversible Data Hiding (RDH), Distortion function, Human Visual System (HVS), Support Vector Regression (SVR), Histogram-Shifting of Prediction Errors (HSPE), Receiver Operating Characteristic (ROC)Iris image, Privacy protection.

1 Introduction

In reality, data hiding has been the subject of many researchers to date. Data hiding, particularly in the context of steganography and covert communication, indeed has three major goals. The first is concealment, to conceal the existence of hidden information within a carrier medium. The second factor is capacity, embedding as much additional data as possible while still maintaining the cover medium's appearance and quality. The final one is robustness, Robustness ensures that the embedded information can be reliably extracted under different conditions [1]. Reversible Data Hiding has recently become more and more significant with increase in

IACIDS 2023, November 23-25, Lavasa, India

DOI 10.4108/eai.23-11-2023.2343227

information security-based applications. RDH is also branded as Lossless Data Hiding (LDH), guarantees both full retrieval of original image and also extraction of (hidden)concealed data, often known as the steganography or watermark. Even though distortion is frequently negligible to Human Visual System (HVS), sensitive applications similar to images and videos cannot accept irreversibility. Because of this, it is envisioned that the RDH will recover the correct host image and hidden(unseen) data [2]. Section 2 highlights Pixel-Based, Block-Based and Interpolation-Based RDH methodologies and was presented as literature review. In Section 3, the methodology of projected Iris Recognition System with RDH using the CASIA-IrisV2, a database for Iris is presented. In Section 4, results and discussions and in section 5 the conclusion is given.

2 Literature Review

As already indicated, the literature has offered a wide variety of ways for Reversible Data Hiding. This research paper's main goals are to survey the RDH methodologies and their key findings discussed in the literatures. Fifty prominent research works have been reviewed and contrasted from this perspective [3]. Best approacehes are categorised into four: pixel-based, block-based, interpolation-based, Quantization and other RDH methods.

Table 1 : Classes of RDH methods

Pixel based	**Block based**	**Interpolation based**	**Quantization**
Pixel modification	Histogram Shifting	Neighbour Mean Interpolation (NMI)	Vector Quantization
Pixel differencing	Mapping	R−weighted Coding Method (RCM)	SMVQ (Side-Matched Vector Quantization)
Arithmetic coding	Authentication		JPEG Q (JPEG Quantization)

Apart from the above-mentioned techniques other Reversible Data Hiding Methods are available. They are Prediction Error Expansion (PEE) Histogram Modification, Steganalysis SVM, Lempel Ziv Welch's High Performance Data Hiding Model (HPDH LZW), Hidden Markov Model (HMM), Artificial Neural Network (ANN), GIS-Vector Maps, Fractal Coding and tamper recognition. However, there is still room for development in terms of the capacity versus imperceptibility trade-off. More capacity is required for some data hiding applications involved in integrity control. The following subsections describe each category of RDH technique in detail. Comprehensively outlined, the difficulties that RDH technique must overcome both image quality and data concealing capability. First the data is encoded, then the

image is partitioned followed by data embedding, later it is decoded and extracted. Pixel-based process deals with shifting, differencing, modification and arithmetic encoding. (Fig.1).

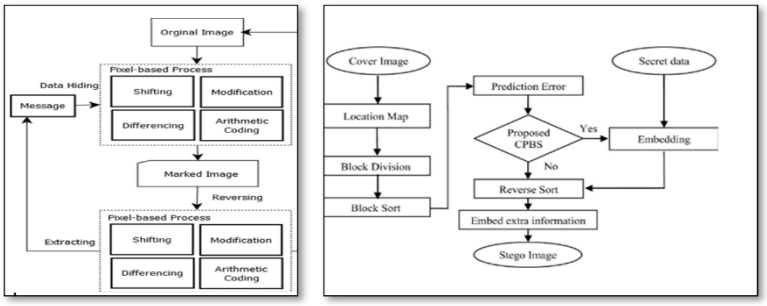

Fig 1. Pixel-Based Techniques used for Reversible Data Hiding System

To overcome the drawback of pixeling, an innovative RDH using Context Pixel Based Block Selection (CPBS) approach is proposed. After block separation, sorting process, the intricacy of every separate block is measured using context pixel that is chosen from current block and also by connected pixels of neighbour block. Experimental results authenticates that projected arrangement accomplishes better capacity distortion trade-off and outperforms with existing PVO(Pixel-value-ordering) techniques [4]. PVO is one of the most popular frameworks in research of RDH in recent years. In furthermost PVO based approaches cover image is divided into non-overlapped blocks to embed secret data into maximum and minimum pixels of each block.

Pixel modification is commonly used in RDH because it allows for a high data embedding capacity while striving to maintain good perceptual quality in the cover image. Pixel modification techniques aim to subtly alter pixel values to encode hidden information while minimizing the perceptual impact on the image. Embedding process is done using LSB Substitution, Prediction Error Coding, Arithmetic Coding and Histogram Modification. The Extraction process reverses the modifications made during embedding to retrieve the original data. Finally, in the reconstruction process, Once the hidden data is extracted, you can reconstruct the original image by reversing any changes made to the pixel values. The prime idea of the method provided in Chang etal - 2007 is changing pixel pairs using confidential data, implied matrix and magic, followed by the creation of two stegno pictures. Stegno pictures enhance visual delivery of security and safeguard private data. Zhang (2011) found that by varying a small content of encrypted data with image, it is possible to hide additional data inside an image after altering content into a cryptographic code, particularly to avoid unauthorised access.

Pixel differencing is a technique used in RDH to embed content or text into digital imageries while preserving ability to perfectly recover original image deprived of any harm of data. Embedding process is done using Pixel Pair Selection, Data Encoding, Difference Calculation and Embedding Data. The Extraction process reverses the modifications made during embedding to recover the original data. Finally, in the reconstruction process, Once the hidden data is extracted, you can reconstruct the original image by reversing any changes made to the pixel differences. After getting the signal passed the authentication operations, Li (2005) used interferences to restore the original signal. The intensity wraps around and low hiding capacity of salt/pepper artefacts, for example, may now be remedied, among other common issues [14].

Tai et al. (2009) presented different Modification Based RDH technique. They employ pixel difference dispersion to achieve a high hiding capacity while minimising distortion, and they also advocate the usage of a Histogram Shifting Technique to prevent underflow & overflow of the pixel. Following a few stages, Celik etal in 2002 apply RDH method. The method first allows for the safe recovery of the innovative host signal through arithmetic coding technique-based subtraction of the encoded information. Then, without sacrificing data embedding capacity, a prediction-based provisory entropy coder boosts compression efficiency by using static sections as side-information [15, 16]. Block-based RDH techniques are commonly used to balance between data hiding size and alteration in host data. These techniques use a box scale grid to represent the pixels, and the grid interacts with the calculation block to modify or shift it. The scheme shown in the Fig.2 illustrates this procedure.

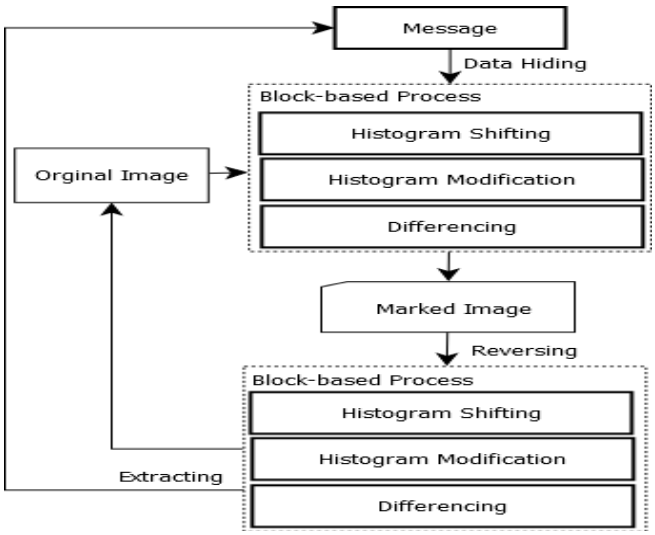

Fig 2a. Block-based data hinding system

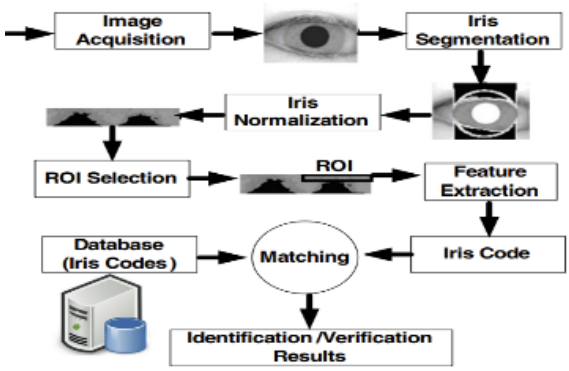

Fig 2b. Iris Segmentation

RDH technique using HSPE (Histogram Shifting of Prediction Errors) employs 2-step erections, prediction stage & Error Modification Stage (EMS) that has apparently remained reported for

the first time by Hong et al. (2008) [5]. Another study on this subject was provided(Kuo etal in 2008) using Block Segmentation technique is the small modification scheme used by Ni et al. (2006) in order to adjust the mechanism used to save data and increase the capacity for data hiding [6, 7]. An RDH approach based on the difference histogram as a result of an empty field for data hiding [8] is also presented by Zeng et al. (2009). Nine fundamental scan paths have been defined, making it possible to acquire all directions surrounding pixel differences. Additionally, Fallahpour et al. (2011) postulate a highly effective method for reversibly masking data based on tiling images and ever-changing histograms of each tile's individual components between the lowest and highest frequency [9]. Zhang's work didn't take benefit of pixels when identifying each block's levelness and did not take into account pixel correlations at edges of vicinal blocks. Hong et al. (2012) have developed an updated version of Zhang's RDH method in converted images. Furthermore, experimental findings put forth by Hong et al. (2012) demonstrate that the proposed method outperforms Zhang's work [10]. Huang et al. (2013) [11] have suggested histogram shifting RDH approach for high bit depth medical image examination. In medical images (Huang etal in (2013)) were able to acquire a strong correlation for the base structure's smooth surface. After hiding data extraction, original image can correctly restore using a converse histogram shifting. This method used by Chen., et al. in 2013 to determine mean value for the minimum Just Ostensible Difference (JND) calculation. JND then develops the ability recognising the proper embedding level to lessen image distortion. [12]. In contrast, Khan et al.'s (2014) suggested histogram processing and block selection (RW-HPBS) solution takes advantage of the idea of down sampling for applications based on control and authentication that require additional capacity [3]. Peak signal two beginning parameters Adaptive Noise Ratio Watermark (ANRW) was chosen based on its statistical features to provide a better visual effect (PSNR) [4].

Histogram modification is a common technique used in Reversible Data Hiding (RDH) to embed extra data while maintaining statistical properties of host data's histogram. The message is hiding within the histogram bin in the work of Ni etal in 2006 histogram-based RDH technique. To achieve low hiding distortion, portions of up and zero points are used, but the hiding capability decreases. The application of the histogram modification technique has also increased recently [7, 13]. Typically rely on tokens, such as ID cards or information such as passwords. The latter runs the risk of being forgotten, while the former is simple to lose and copy. As a result, biometric authentication technology has lately undergone significant development [18]. Multi-modal biometric data is protected via multi-layer watermarking and steganography by Whitelam et al. The iris prototype data in [19] is solely entrenched in the blue channel. Although, these techniques conceal biometric image data with a respectable level of performance. There is yet no solution on how to lessen the effect of data embedding on biometric recognition. STC[14] pattern for Iris data hiding is used in this paper, using a STC for RDH in iris images involves embedding additional data into the iris image while preserving the ability to perfectly recover the original iris data during extraction. Another reversible data hiding method is provided by Yalman et al. (2010) and is based on the 'R-Weighted Coding Method' (RCM) and 'Neighbour Mean Interpolation' (NMI) method [14]. Yalman and Akar (2014) propose the Neighbour Mean Interpolation (NMI) approach and the R-weighted Coding approach (RCM) as the foundation for their High Capacity Reversible Data Hiding (HCR Hide) method [17]. Results from a combination evaluation of noiselessness and data-hiding capacity have shown that suggested method outperforms existing Reversible Data Hiding (RDH) techniques. The findings of new technique have validated the suggested method's superior performance to the current reversible data hiding methods.

3 Materials and Methods

An iris image data concealing approach is projected in this paper. Utilising STC-based content concealing, private information integrated into an iris image. By conveying a high entrenching charge to the zone with significant features of Iris, a unique distortion function is suggested to reduce the effect of embedded information on iris recognition. The capability of the eye-Iris Identification system is evaluated using the CASIA - IrisV2 dataset of iris features [21]. For testing, 60 classes were selected, ten images per class & a total number of six hundred, 640x480 Bit Map pictures.

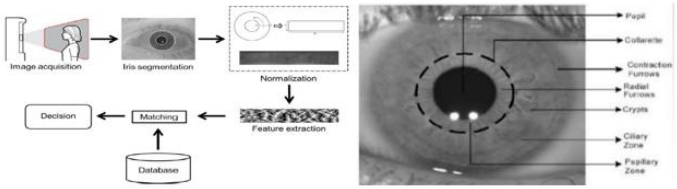

Fig 3. Frontview of eye and Features of Iris

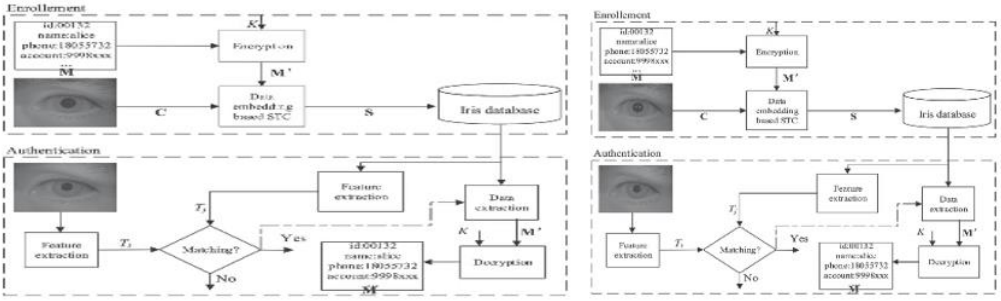

Fig 4. Iris Biometric Authentication System for RDH

The iris authentication mechanism taken into account in this paper is depicted in Fig. 4. Using known encryption methods, such as the DES “Data Encryption Standard” and IDEA “International Data Encryption Algorithm” with a key K that acts as embedding key, the personal data “M” first encrypted to cypher text M’ during the enrolment process. The secret data-containing iris image S is then created by embedding M into a recorded eye-iris image “C” using suggested entrenching technique. Iris database then stores S for authentication. An iris image is processed in the authentication phase to produce a unique code for iris “Ti”. Additional iris code, “Tj”, then taken from its database's iris and is utilised to perform authentication through matching. When identical score exceeds the system-set threshold, the matching is considered successful. When the matching is successful, the cypher text M’ is retrieved from given image. User then receives personal privacy data M next to decryption using the similar key K. The private information will not be extracted if the matching fails. RDH can offer these benefits, it also presents technical challenges, such as achieving the right balance between context capacity, visual and biometric quality of iris. Additionally, security measures must be in place to shelter the entrenched data and avert unlicensed access or tampering. Careful design and adherence to ethical and legal guidelines are essential when implementing RDH with STC

in iris recognition systems. Syndrome Trellis Code is used for embedding the data in suggested method. In case where i is equal to 1, 2 till k and j is 1, 2 upto l, represent the size of cover image (k X l), then (i, j)th element is represented as c(i, j) & cost for embedding is allocated for c(i,j) used as ρ(i, j). The embedding capacity has negligible steganography Distortion, D of the stegno image with 'm' bits. A novel distortion function is suggested to lessen effect that embedding has on the ability to recognise an iris. The distortion function is designed in two basic steps. First, preliminary entrenching cost is generated for each element of image using clever edge detection technique [20]. The embedding cost is then adjusted using the image's gradient. First, cover image's gradient values, which reproduces the fluctuating magnitude in different paths are determined. c(i, j)'s gradient is denoted as Gx(i,j) horizontal direction and Gy(i,j) in vertical direction. Equations (6) and (7) are used to determine the 3-neighbour's mean values Gh(i, j) and Gv(i, j) of the gradient for c(i, j) in the both directions. For the areas with significant iris features, the suggested distortion function consigns substantial embedding costs. The influence of embedding on iris recognition is reduced when combined with STC.

Algorithm:

Embedding data into iris images using the Syndrome-Trellis Code (STC) for Reversible Data Hiding (RDH) is a complex process that involves several steps. Below are the algorithmic steps for RDH using STC in the context of iris images:

Step 1 : Image Selection: Choose the iris image that will serve as the cover image for data embedding. Ensure that the selected image is of high quality and suitable for biometric purposes.

Step 2 : Data to Embed: Prepare the additional data to be embedded into Iris. It could be any supplementary information or metadata that is to be associated with the iris data.

Step 3 : Data Pre-processing: Pre-process the additional data (if necessary) to ensure it is suitable for embedding.

Step 4 : Edge Detection: Apply any edge detection algorithm to the iris image to extract its edge information.

Step 5 : Syndrome-Trellis Code Selection: Choose a suitable STC for the embedding process. The STC is used to encode the iris data in a manner that allows for reversible embedding and extraction.

Step 6 : Data Encoding: Encode the original iris data using the chosen STC. This encoding process generates syndromes that will be used for verifying the integrity of the iris data during extraction.

Step 7 : Data Embedding Strategy: Define the strategy for embedding the additional data into the edge map generated by edge detection. It is chosen to embed data in specific edge points or in the edge strength values, depending on the application.

Step 8 : Embedding Process: Embed the additional data into the selected edge points or edge strength values of the edge map. This typically involves modifying pixel values in the edge map to carry the hidden information. Ensure that the changes are carefully controlled to minimize perceptual distortion.

Step 9 : Reversibility and Data Integrity: Ensure that the embedding process is designed to be reversible, allowing for well defined extraction of both original iris & embedded data without any loss or distortion.

Step 10 : Data Extraction: During extraction, identify the embedded data ie., extract the embedded data using the reverse process.

Step 11 : Decode Embedded Data: If the embedded data was encoded or encrypted before embedding, decode or decrypt it to retrieve the original message or information. Use the extracted data and the original iris data to reconstruct the complete iris data.

Step 12 : Integrity Verification: Verify the integrity of the recovered iris data by comparing it with the original iris data's syndromes. If they match, the data is considered intact; otherwise, there may have been unauthorized modifications.

Implementation of this algorithm requires a deep understanding of image processing, data hiding techniques, syndrome-trellis codes and iris recognition systems. Additionally, the specific techniques and parameters used will depend on the application's requirements and the acceptable trade-offs between capacity, distortion, and security.

4 Results & Discussion

The capability of the recognition system of Iris, is evaluated using the CASIA-IrisV2 iris dataset [21]. For testing, 60 classes were selected, ten images per session, and a total number of six hundred, 640x480 Bit Maps. These iris images are used as cover image, data are embedded and extracted using code in python 3.11 and checked for Reversible Data Hiding.

4.1 Embedding Cost

Embedding costs determined on iris picture (highlighted in white color) are shown in Fig. 5. The embedding cost is cheaper and the alteration capability is greater for brighter marks and lesser for dull marks. Non-edge part(represented by black color), has an endlessly low embedding cost. The iris region identified using the above-mentioned procedure is shown in Fig. 6.

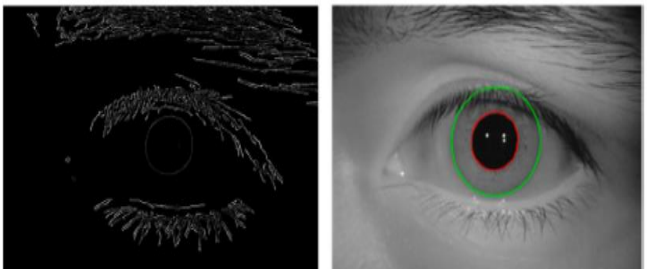

Fig 5: Iris adaptability indication with embedding cost in the iris area detected

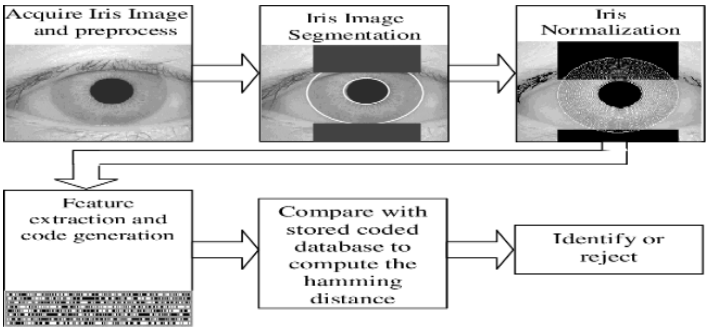

Fig 6: Iris Recognition System with pre-processing, segmentation and normalisation

4.2 Iris Reconition Rate

Matching score is determined during authentication by comparing the iris with associated iris images in the dataset. The prospect that two are from the same person increases with the matching score. To evaluate the effectiveness of iris recognition, a Receiver Operating Characteristic (ROC) curves is used. SMR(Successful Match Rate) and FAR(False Accept Rate) ROC curves are plotted. The ratio of matching false scores are higher or equals the threshold, known as the FAR. Purpose of embedding, personal private data using a pseudo-random number generator is intimated. The request is done to match related photos in the dataset with iris images devoid of personal information produces the scores of matching. Suggested approach employs non-STC based entrenching procedures EMD[22], matrix embedding as well as the STC based HILL[19], S-UNIWARD[18], and HUGO [16] are used to implant data using a 0.15bits per pixel payload.

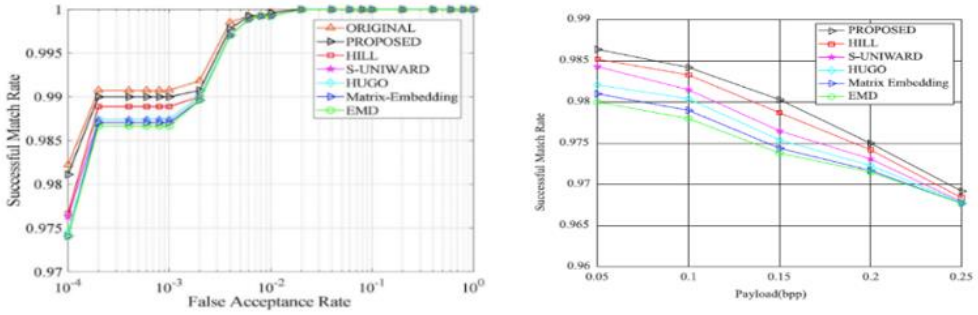

Fig 7. ROC curves with different embedding algorithms in graph format

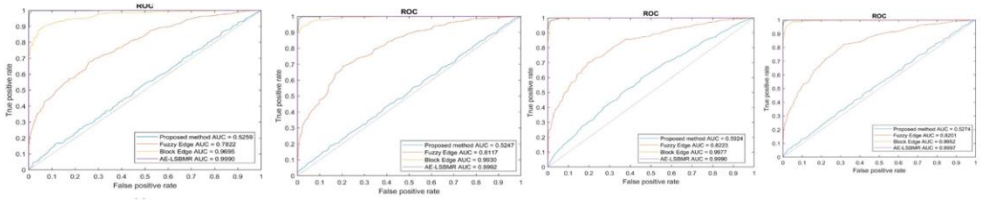

Fig 8. Comparisons of recognition rate with FAR

Fig.7 presents the ROC curves. The unique ROC curve, deprived of any embedding operations are also presented for comparison's sake. It is clear that the identification rate performs slightly worse under the suggested technique. Image content is also taken into account and so, STC-based embedding algorithms provide greater recognition rates when compared to non-STC-based embedding algorithms. Additionally, the proposed method outperforms all embedding methods in the terms of recognition rate because of the suggested Distortion function created under direction of recognition rate. The possibility of having personal information incorporated in the iris feature region might reduce the accuracy of iris identification. The benefit of the suggested strategy is no longer immediately apparent in this situation. Since the payload is greater than 0.2 bpp, the recognition rates of the various approaches are comparable.

5 Conclusion

Data Hiding for iris is proposed here. Reversible Data Hiding (RDH) using Syndrome-Trellis Codes (STC) is a powerful technique that allows for the secure and efficient embedding of additional data within digital media while ensuring reversibility and data integrity. Privacy of users is sustained; private information is added up with iris. The results demonstrate that it has the ability to maintain a high level of recognition accuracy while embedding enough personal information into the iris image. RDH with STC allows for an increase in data capacity within iris images without compromising the original biometric data's quality. The use of STC ensures that the embedding process fully reversible. Both original iris data and embedded data can be extracted without loss or distortion, maintaining the reliability of iris. Various biometric image data concealing techniques can be considered for additional research.

References

[1] A. G. Gale1, DR. S. S. Salankar, "A Review on Advance Methods of Feature Extraction In Iris Recognition System", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 22781676, p-ISSN: 2320-3331 PP 65-70, International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014)

[2] M. H. Hamd,"Optimized biometric system-based iris-signature for human identification", International Journal of Advances in Intelligent Informatics ISSN 2442-6571 Vol. 5, No. 3, November 2019, pp. 273-284

[3] Murat Kuslu, Yildiray Yalman, Contemporary Approaches on Reversible Data Hiding Methods: A Comparative Study, International Journal of Applied Mathematics, Electronics and Computers Advanced Technology and Science ISSN: 2147-82282, IJAMEC, 2016, 4(1), 1-9, 2013

[4] C. Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li., 2006. An Improved Reversible Data Hiding Using Pixel Value Ordering and Context Pixel-Based Block Selection, In the Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), pp:873-877,https://link.springer.com/chapter/10.1007/978-981-15-3369-3_64,DoI :10.1007/978-981-15-3369-3_64

[5] Enas N. Jaara, Iyad F. Jafar , Reversible Data Hiding Based on Histogram Shifting of Prediction Errors Using Two Predictors, 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), 978-1-4799-7431-3/15-2015 IEEE

[6] C D Divya and A B Rajendra, “Review on the proportional study of segmentation techniques for iris acknowledgment”, International Conference on Research Frontiers in Sciences (ICRFS 2021) Journal of Physics: Conference Series, 1913 (2021) 012096, IOP Publishing doi:10.1088/1742-6596/1913/1/012096

[7] Kuo, Wen-Chung, Jiang, Dong-Jin, Huang, Yu-Chih, "A Reversible Data Hiding Scheme Based on Block Division", Doi:10.1109/CISP.2008.730, 1st International Congress on Image and Signal Processing, CISP 2008, 365-369, IEEE

[8] Hanaa M. Ahmed a , Mohammed A. Taha, A Brief Survey on Modern Iris Feature Extraction Methods, Engineering and Technology Journal, Vol. 39, Part A (2021), No. 01, Pages 123-129

[9] Hashim M. M., Taha M. S., Aman A. H. M., Hashim A. H. A., Rahim M. S. M., & Islam. S, Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography, 2019 7th International Conference on Mechatronics Engineering (ICOM), 978-1-7281-2971-6/19/2019 IEEE
[10] Zhang X., Qian Z., Feng G., & Ren, Y. (2014). Efficient reversible data hiding in encrypted images. Journal of Visual Communication and Image Representation, 25(2), 322–328. Science Direct, Elsevier 2013.
[11] Yang Yang, Weiming Zhang, Dong Liang, Nenghai Yu, A ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images, Multimed Tools Appl, Springer Science+Business Media New York 2017
[12] Wenbo Wan , Jun Wang , Yunming Zhang , Jing Li, Hui Yu, Jiande Sun, A comprehensive survey on robust image watermarking, Neurocomputing, Volume 488, 1 June 2022, Pages 226-247, Elsevier
[13] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification, IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, JULY 2013, IEEE
[14] Guo-Dong Su, Yanjun Liu, Chin-Chen Chang, A square lattice oriented reversible information hiding scheme with reversibility and adaptivity for dual images, doi:10.1016/j.jvcir.2019.102618, 1047-3203/ 2019 Elsevier Inc
[15] Chia-Chen Lina,∗, Wei-Liang Taib, Chin-Chen Chang, Multilevel reversible data hiding based on histogram modification of difference images, Pattern Recognition, 41(12), 3582–3591. doi:10.1016/j.patcog.2008.05.015, Elsevier
[16] Silveira, D., Povala, G., Amaral, L., Zatt, B., Agostini, L., & Porto, M. (2015). Efficient reference frame compression scheme for videocoding systems: algorithm &VLSI design. Journal of Real-Time Image Processing.doi:10.1007/s11554-015-0551-1,Cross Mark Pub.,
[17] Malik, A., Sikka, G., & Verma, H. K. (2016). Image interpolation based high capacity reversible data hiding scheme. Multimedia Tools and Applications, 76(22), 24107–24123. doi:10.1007/s11042-016-4186-4, 2016, Springer
[18] Kunal Kumar, Mohammed Farik , A Review Of Multimodal Biometric Authentication Systems, International Journal Of Scientific & Technology Research Volume 5, Issue 12, DECEMBER 2016 ISSN 2277-8616, IJSTR
[19] Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A safe and secured iris template using steganography and cryptography. Multimedia Tools and Applications. doi:10.1007/s11042-020-08971-x, Springer
[20] Sheng Li, Xin Chen, Zichi Wang, Zhenxing Qian and Xinpeng Zhang, Data Hiding in Iris Image for Privacy Protection, IETE TECHNICAL REVIEW2018, VOL. 35, NO. S1, 34–41https://doi.org/10.1080/02564602.2018.1520153, 2018
[21] A. Singh, A. Pandey, M. Rakhra, D. Singh, G. Singh and O. Dahiya, "An Iris Recognition System Using CNN & VGG16 Technique," 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2022, pp. 1-6, doi: 10.1109/ICRITO56286.2022.9965172.
[22] Ali Athar, Alexander Hermans, Jonathon Luiten, Deva Ramanan, Bastian Leibe; TarViS: A Unified Approach for Target-Based Video Segmentation, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, pp. 18738-18748,
https://openaccess.thecvf.com/content/CVPR2023/html/Athar_TarViS_A_Unified_Approach_for_Target-Based_Video_Segmentation_CVPR_2023_paper.html