An Improved Algorithm For Bio Metric Based Secret Data Hiding

Dr.M.Kavitha[1], R.Archana[2], R.Deepika[3], K.Iswarya[4]
[1]Professor, Dept of ECE
[2, 3, 4]Dept of ECE
[1, 2, 3, 4] K.Ramakrishnan college of Technology, Trichy

Abstract- *Sparse representation is used for compression process. For a replacement given fingerprint images, represent its patches consistent with the dictionary by computing l0-minimization then quantize and encode the representation. Experiments also illustrates that the algorithm is robust to extract minutiae. This algorithm is efficient compared with JPEG, JPEG 2000 and WSQ. All previous methods have compressed fingerprint images. After that compressed images two finger combination based new finger print create for top secure privacy protection. A novel system for shielding fingerprint privacy by combining two different fingerprints into a replacement identity for authentication. And also to classify the training samples should include fingerprints with different quality ("good", "bad", "ugly"). Data hiding usually involves the alteration of a canopy signal for embedding a secret message. This scheme doesn't need any cover signals to participate. Instead, it generates the finger vein image based on a piece of hologram phase constructed from the secret message. The hologram phase consists of the spiral phase and therefore the continuous phase. The secret message can be extracted by detecting the encoded points in the constructed finger vein. . It is also difficult to detect the existence of secret message from the constructed finger vein image.*

I. INTRODUCTION

Data hiding is a technique of embedding a secret message into a cover signal by subtly altering selected locations. It is widely applied in authentication, secure communication and copyright protection.Generally speaking, the cover signal could be any meaningful digital signal including the digital audio/image/video text and even the 3D meshes. Among various data hiding techniques, image based data hiding is the most popular, where the cover signal is a digital image such as a natural image a medical image.Image based data hiding can be developed for images in different forms, including color/grayscale images and binary images.Most of the existing image based data hiding techniques require a cover image to participate.The pixels of the cover image will be modified to host the secret message, which inevitably causes distortions visually or statistically. Thus, it is possible to develop steganalysis tools to reveal the existence of the secret message in the stego-images.

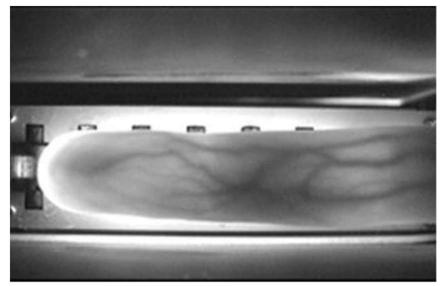


Fig.1:finger vein representation image

II. FINGER VEIN SYNTHESIS.

Data hiding could also be a software development technique specifically utilized in object-oriented programming (OOP) to hide internal object details (data members).

Data hiding could also be a software development technique specifically utilized in object-oriented programming (OOP) to hide internal object details (data members). Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended changes.

Data hiding is additionally mentioned as data encapsulation or information hiding. Data hiding was introduced as a neighborhood of the OOP methodology, during which a program is segregated into objects with specific data and functions.

B. FINGER VEIN A finger vein is an impact left by the friction ridges of a person's finger. The recovery of partial fingerprints from a criminal offense scene may be a crucial method of forensic science. Moisture and grease on a finger end in finger veins on surfaces like glass or metal. Human finger vein are detailed, nearly unique, difficult to vary , and durable over the lifetime of a personal , making them suitable as long-term markers of human identity.

Before computerization, manual filing systems were utilized in large finger vein repositories. A finger vein arrangement groups finger vein consistent with their characteristics and thus helps within the matching of a finger vein against an outsized database of finger vein.

Finger vein that must be matched can therefore be compared with a subset of finger vein in an existing database. Early classification systems were supported the general ridge patterns, including the presence or absence of circular patterns, of several or all fingers. This allowed the filing and retrieval of paper records in large collections supported friction ridge patterns alone. the foremost popular systems used the pattern class of each finger to form a numeric key to assist lookup during a filing system . Finger vein classification systems included the Roscher System, the Juan Vucetich System and therefore the Henry arrangement .The Henry arrangement was developed in India and implemented in most English-speaking countries. within the Henry arrangement there are three basic finger vein patterns: loop, whorl, and arch, which constitute 60–65 percent, 30–35 percent, and 5 percent of all finger vein respectively.[citation needed] .

C.THE PHASE REPRESENTATION OF FINGER VEIN

The system employed by most experts, although complex, is analogous to the Henry arrangement . It consists of 5 fractions, during which R stands for right, L for left, i for index , m for finger , t for thumb, r for annualry and p(pinky) for little finger.

The fractions are as follows:
The fractions are as follows:

Ri/Rt + Rr/Rm + Lt/Rp + Lm/Li + Lp/Lr

The numbers assigned to every print are supported whether or not they're whorls. A whorl within the first fraction is given a 16, the second an 8, the third a 4, the fourth a 2, and 0 to the last fraction. Arches and loops are assigned values of 0. Lastly, the numbers within the numerator and denominator are added up, using the scheme:

For example, if the proper annualry and therefore the left index have whorls, the fraction used is:

0/0 + 8/0 + 0/0 + 0/2 + 0/0 + 1/1

The resulting calculation is:

(0 + 8 + 0 + 0 + 0 + 1)/(0 + 0 + 0 + 2 + 0 + 1) = 9/3 = 3

The flexibility of friction ridge skin means no two finger or palm vein are ever exactly alike in every detail; even two impressions recorded immediately after one another from an equivalent hand could also be slightly different.[citation needed] Finger vein identification, also mentioned as individualization, involves an expert, or an expert computing system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to possess originated from an equivalent finger or palm (or toe or sole). An intentional recording of friction ridges is typically made with black printing ink rolled across a contrasting white background, typically a white card. Friction ridges also can be recorded digitally, usually on a glass plate, employing a technique called Live Scan. Latent prints are invisible to the eye , whereas "patent prints" or "plastic prints" are viewable with the unaided eye. Latent prints are often fragmentary and need the utilization of chemical methods, powder, or alternative light sources so as to be made clear. Sometimes a standard bright flashlight will make a latent print visible.

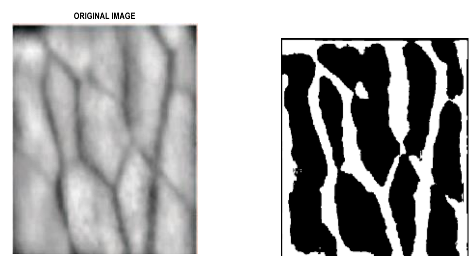


Fig.2(a)original image,(b)minutiae image

Factors which affect the standard of friction ridge impressions are numerous. Pliability of the skin, deposition pressure, slippage, the fabric from which the surface is formed , the roughness of the surface, and therefore the substance deposited are just a few of the various factors which may cause a latent print to seem differently from any known recording of an equivalent friction ridges For these reasons, finger vein examiners are required to undergo extensive training. The scientific study of finger vein is called dermatoglyphics.

Finger vein can be captured as graphical ridge and valley patterns. Because of their uniqueness and permanence, finger vein emerged as the most widely used biometric identifier in the 2000s. Automated finger vein verification systems were developed to meet the needs of law enforcement and their use became more widespread in civilian applications. Despite being deployed more widely, reliable automated finger vein verification remained a challenge and was extensively researched in the context of pattern recognition and image processing. The uniqueness of a finger vein can be established by the overall pattern of ridges and valleys, or the logical ridge discontinuities known as minutiae. In the 2000s minutiae features were considered the most discriminating and reliable feature of a finger vein. Therefore the recognition of minutiae features became the most common basis for automated finger vein verification. The most widely used minutiae features used for automated finger vein verification were the ridge ending and the ridge bifurcation.

III. FINGER VEIN IMAGE CONSTRUCTION

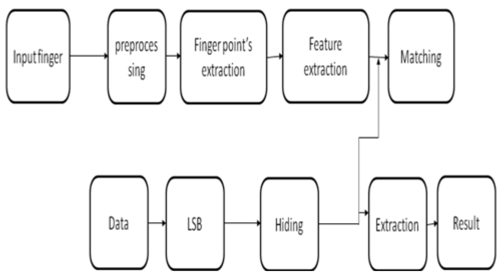


Fig.3:block diagram representation of finger vein recognition and secret message hiding technique

A.SPIRAL PHASE CONSTRUCTION

In order to construct the spiral phase, we propose to encode the secret message s into a set of n two dimensional points {(xi, yi)} n i=1 with the corresponding polarities {pi} n i=1. The basic idea is to map the secret message to a polynomial. Then, we evaluate the polynomial on n different elements over a Galois field to compute xi , yi and pi, as shown in Fig. 5. The details of the encoding process are summarized below.

1) Compute a set of cyclic redundancy check (CRC) bits according to s, which is used for error detection during data extraction.
2) Partition s into a group of k symbols with r bits per symbol:
3) Evaluate the polynomial ℘k over the Galois field F = G F(2r) at n (n ≥ k) different elements
4) Map the points P to a set of encoded spirals

In other words, we can fix the width and height of the fingerprint image and determine the value of n and r. As long as n ≥ k, secret messages with different length (i.e., different k) can be encoded to form a set of n encoded spirals, where more redundancy (i.e., n −k spirals) will be added for shorter.

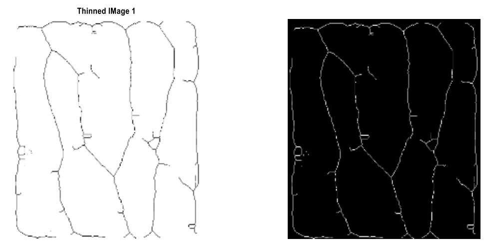


Fig.4(a)thinning image,(b)termination image

C. POST PROCESSING

With the constructed spiral phase ψs and continuous phase ψc, the composite phase ψ of the constructed fingerprint is computed by combining them together according to Eq. (5). During the phase combination, the local fingerprint orientation will be slightly changed (when compared with Oκ) due to the creation of minutiae points. According to the model given in Eq. (1), the phase modulated signal cos(ψ) represents an ideal fingerprint, while the other components just make the fingerprint to be realistic. The gradual change of the cosine wave forms the fingerprint ridges and valleys. The value of the composite phase also gradually increases or decreases from (0, 2π] or [2π, 0) within two consecutive ridges as shown in Fig. 10. This property makes it easy to obtain a binary fingerprint image directly from ψ using a single threshold. Concretely, a binary fingerprint image Fb can be computed by

$$Fb(x, y) = \{1 \text{ i f } \psi(x, y) > \tau$$

$\{ 0$ otherwise,

where $\tau \in (0, 2\pi)$ is the threshold to construct the binary fingerprint image. The value of τ controls the thickness of the fingerprint ridges. It can be seen from Fig. 11 become thinner when τ decreases.

We set $\tau = \pi$ to obtain the final binary fingerprint image and $\tau = 0.4\pi$ to get a coarsely thinned fingerprint image. Please refer to Section VI-A for the settings of τ . The final thinned fingerprint image is constructed by iteratively removing the boundary pixels from the coarsely thinned fingerprint image using the algorithm proposed in [42] (see Fig. 12(a)). To construct the grayscale fingerprint image, we treat the binary fingerprint image as the master fingerprint. Then, as suggested in [27], we perform noising on the master fingerprint by adding small white blobs of various sizes and shapes (see Fig. 12(b)). The post processing hardly affects the locations of the fingerprint minutiae, as shown in Fig. 10, Fig. 11, and Fig. 12. This is to say, the spirals of the constructed fingerprint, which encode the secret message, will be very close before and after the post processing. Please refer to

Section VI-A for quantitative measures of the distortion of the constructed finger vein before and after processing..

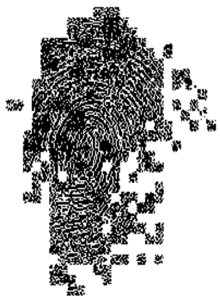
RESULTS AND DISCUSSION:

3.3 Proposed method results and analysis

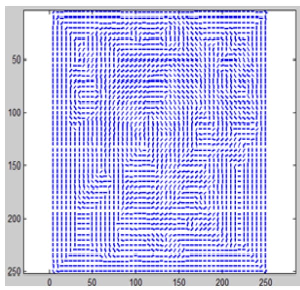
3.3.1.1Fingerprint combination for privacy protection

Enrollment section

Reference Points and minutiae position extraction

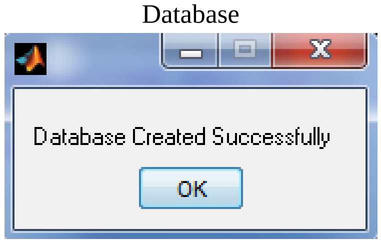


Reference Points and orientation extraction



Combined minutiae template

Database

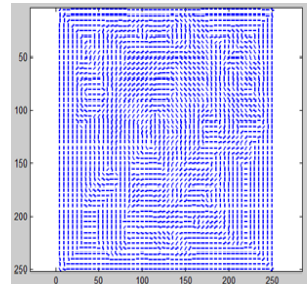


3.3.1.1Privacy protection protection based Authentication

Authentication section

Reference Points and minutiae position extraction

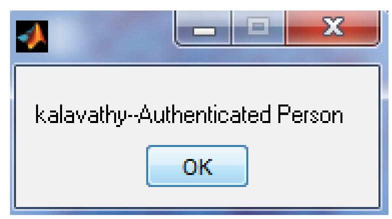
Reference Points and orientation extraction



Fingerprint matching

Minutiae image from authentication

Database image



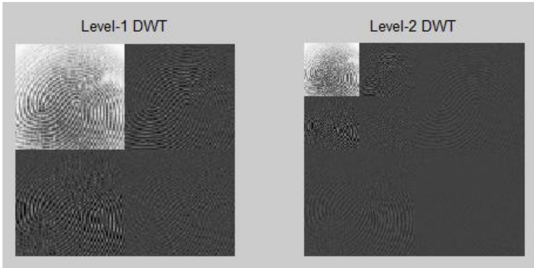
3.3.2 Finger print Classification

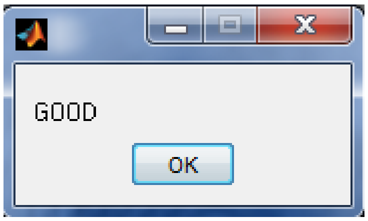
Input image

compressed image

Feature extraction

Two level biorthogonal wavelet Result





D.CONCLUSION

A novel construction based data hiding technique is proposed in this paper. Instead of constructing textures as what have been done in the literature, we propose to construct fingerprint images directly from the secret message. The proposed scheme is based on the construction of the composite phase of the fingerprint, which is the combination of the spiral phase and the continuous phase. The spiral phase is constructed by encoding the secret message to a set of two dimensional points with different polarities, while the continuous phase is constructed from a fingerprint image synthetically generated. Different fingerprint images can be generated based on the constructed composite phase, including the binary fingerprint image, the thinned fingerprint image, and the grayscale fingerprint image. The experimental results show that our scheme achieves satisfactory data extraction accuracy and robustness. In addition, we demonstrate the ineffectiveness of the existing steganalysis tools on the constructed finger vein images. The average detection error is 35.25% and 31.20% for detecting the constructed fingerprint images from the pure synthetic fingerprint images and the original fingerprint images, respectively. This demonstrates the usefulness of the fingerprint specific features for steganalysis. In the future, the traces left due to the fingerprint construction should be further studied to improve the performance of steganalysis. Meanwhile, a better spiral phase construction approach should be investigated by putting proper constraints on the distribution of the encoded spirals.

REFERENCES

[1] Jain, A.K.; Ross, A.; Pankanti, S. Biometrics: A Tool for Information Security. IEEE Trans. Inf. Forensics Secur. 2006, 1, 125–143.

[2] Goode Intelligence. Biometrics—The Must-Have Tool for Payment Security. 2015. Available online: https://www.goodeintelligence.com/wp-content/uploads/2016/11/Goode-Intelligence-White-PaperBiometrics-the-must-have-tool-for-payment-security.pdf (accessed on 4 August 2019).

[3] IBM Security. Future of Identity Study. 2018.

[4] Unar, J.; Seng, W.C.; Abbasi, A. A review of biometric technology along with trends and prospects. Pattern Recognit. 2014, 47, 2673–2688.

[5] Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 2004, 14, 4–20.

[6] Jain, A.K.; Kumar, A. Biometric Recognition: An Overview. In Second Generation Biometrics: The Ethical, Legal andSocialContext; Mordini, E., Tzovaras, D., Eds.; Springer: Dordrecht, Netherlands, 2012; pp. 49–79.

[7] Peralta, D.; Galar, M.; Triguero, I.; Paternain, D.; García, S.; Barrenechea, E.; Benítez, J.M.; Bustince, H.; Herrera, F. A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. Inf. Sci. 2015, 315, 67–87.

[8] Prasad, P.S.; Devi, B.S.; Reddy, M.J.; Gunjan, V.K. A Survey of Fingerprint Recognition Systems and Their Applications. In Proceedings of the International Conference on Communications and Cyber Physical Engineering 2018, Hyderabad, India, 24–25 January 2018; pp. 513–520.

[9] Abate, A.F.; Nappi, M.; Riccio, D.; Sabatino, G. 2D and 3D face recognition: A survey. Pattern Recognit. Lett. 2007, 28, 1885–1906.

[10] Mahmood, Z.; Muhammad, N.; Bibi, N.; Ali, T. A review on state-of-the-art face recognition approaches. Fractals 2017, 25, 1750025.

[11] Daugman, J. How iris recognition works. IEEE Trans. Circuits Syst. Video Technol. 2004, 14, 21–30. 12. Patil, S.; Gudasalamani, S.; Iyer, N.C. A Survey on Iris Recognition System. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 2207–2210.

[12] Kong, A.; Zhang, D.; Kamel, M. A survey of palmprint recognition. Pattern Recognit. 2009, 42, 1408–1418.

[13] Zhong, D.; Du, X.; Zhong, K. Decade progress of palmprint recognition: A brief survey. Neurocomputing 2019, 328, 16–28.

[14] Lawson, A.; Vabishchevich, P.; Huggins, M.; Ardis, P.; Battles, B.; Stauffer, A. Survey and Evaluation of Acoustic Features for Speaker Recognition. In Proceedings of the 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),

Prague, Czech Republic, 22–27 May 2011; pp. 5444–5447.

[15] Hansen, J.H.; Hasan, T. Speaker recognition by machines and humans: A tutorial review. IEEE Signal Process. Mag. 2015, 32, 74–99.

[16] Shaheed, K.; Liu, H.; Yang, G.; Qureshi, I.; Gou, J.; Yin, Y. A systematic review of finger vein recognition techniques. Information 2018, 9, 213.

[17] Soh, S.C.; Ibrahim, M.; Yakno, M. A Review: Personal Identification Based on Palm Vein Infrared Pattern. J. Telecommun. Electron. Comput. Eng. 2018, 10, 175–180.

[18] Wan, C.; Wang, L.; Phoha, V.V. A survey on gait recognition. ACM Comput. Surv. 2018, 51, 89.

[19] Connor, P.; Ross, A. Biometric recognition by gait: A survey of modalities and features. Comput. Vis. Image Underst. 2018, 167, 1–27.

[20] Deore, M.R.; Handore, S.M. A Survey on Offline Signature Recognition and Verification Schemes. In Proceedings of the 2015 International Conference on Industrial Instrumentation and Control (ICIC), Pune, India, 28–30 May 2015; pp. 165–169.

[21] Kutzner, T.; Pazmiño-Zapatier, C.F.; Gebhard, M.; Bönninger, I.; Plath, W.D.; Travieso, C.M. Writer Identification Using Handwritten Cursive Texts and Single Character Words. Electronics 2019, 8, 391.