Secured ICA Technique on Bimodal Biometric Images Using Private Watermarking with DCT

Umasankari N<sup>a</sup> and Muthukumar B<sup>b</sup>

<sup>a</sup>Research Scholar, Dept of IT, Sathyabama Institute of Science and Technology, India
<sup>b</sup>Professor, Dept of CSE, Mohamed sathak AJ college of Engineering, Chennai

Abstract. With the discovery of paperless expensive means of internet access, network communication via social media is on the rise, which often comprises threats and distortions. Un authenticates identification may sometimes lead to ambiguities in end-user identification and misunderstandings. Therefore, proper identification of a person is a must in network communication. Image private watermarking<sup>7</sup><sup>9</sup><sup>19</sup> is one solution when the owner of the digital images are identified properly by embedding additional information such as a private watermark in the digital images like fingerprint and retina imperceptibly concealed inside another image. On the other hand, communication also leads to a serious surge in decompress technique on the images. This work introduces three techniques: digital watermarking, steganography, ICA<sup>4</sup><sup>5</sup><sup>6</sup><sup>20</sup><sup>22</sup>. Using a private watermark using the visible <sup>9</sup><sup>7</sup> and non-blind<sup>9</sup><sup>19</sup><sup>7</sup> technique on the photo image. Then two original fingerprints and retina images to achieve stego analysis technique to convert as a stego image. Then the stego image concealed by a watermarked photo image. Then mixing the two techniques to achieve the ICA<sup>20</sup><sup>22</sup><sup>4</sup><sup>5</sup><sup>6</sup> (Independent Component Analysis) for protecting data transmission. To providing compression using the IDCT (Inverse Discrete Cosine Transform) technique with the key using AES<sup>10</sup><sup>9</sup><sup>19</sup> (Advanced Encryption Standard) 64-bit algorithm. Implementation and to determine the utilize the JAVA platform.

Keywords. AES, DOS, Fingerprint, IDCT, ICA, IEEE 802.15.4., MAC, Multimodal, Private Watermark, Retina, Steganography.

1. Introduction

As we beat the current model challenges like age cause for utilizing biometric pictures for physical characteristics and Query Based biometric system<sup>17</sup><sup>18</sup>. Cryptography and steganography<sup>9</sup><sup>19</sup> are cousins in the spycraft family. Cryptography<sup>9</sup><sup>19</sup> and Steganography<sup>1</sup><sup>3</sup><sup>12</sup><sup>13</sup> are frequently interrelated and share the shared objectives and administrations of securing the classification, trustworthiness, and accessibility of data. In the cryptosystems model, the interloper predicts some time information might be hidden<sup>1</sup><sup>3</sup><sup>8</sup>. Expanding the procedure of cryptography may give security at times utilizing a wide range of vigorous calculations. As we keep in our mind kerchoffs’ standards at whatever point we plan the model each saltine is extremely more grounded than against our characterized models to break the whole

---

1 Umasankari N, Research Scholar, Dept of IT, Sathyabama Institute of Science and Technology, India
Email: san_june18@yahoo.com
frameworks will be crumpled and take our significant data. Figure 1 discloses the above chart to concealed verified biometric[8][14] pictures through the steganography[12][13] system. This watermark is utilized for verification purposes.

![Figure 1. Generic Steganography Representation](image)

2. Secured Steganography and Biometric System

2.1. History of Steganography

Chinese composed messages on silk and encased them in chunks of wax. At that point wax ball, "la wan", could then be hidden[1] in the delegate. An increasingly unpretentious strategy, almost as old, is to utilize undetectable ink (lemon juice, milk, or pee, all of which turn dull when held over a fire). Unique "inks" were significant steganographic[1][3][8] tools in any event, during the Second World War. The extraordinary man Nethaji Subhash Chandra Bose time. A portion of his devotees holds his photograph is denied and serious discipline, at the time of the 1940s. So the supporter draws the blending of two pictures Subhash Chandra Bose and India map including Barath matha. The best approach to can see the Subhash Chandra Bose picture collapsing paper in certain ways. The supporter just realizes how to overlay the paper cause it to show up his picture on the paper. The outsider can't see bose picture and furthermore didn't have the foggiest idea about the collapsing strategy for paper. Here one of the example episodes before free utilized this system in a significant way.

2.2. Modern Steganography

Steganograpy[1][3][8][14] is the word is of Greek inception and signifies "disguised composition" from the Greek word steganos signifying "secured or ensured", and graphe signifying "composing". "Steganography implies concealing one bit of information inside another". In prior days the incomparable fear monger Bin Laden is Steganography Master; it's when Osama receptacle Laden begins utilizing the Internet. The USA-container Laden and others "are concealing maps and photos of fear monger targets and posting directions for psychological militant exercises on sports visit rooms. The strategy, known as steganography, is the act of installing mystery messages in different messages in a way that keeps an onlooker from discovering that anything abnormal is occurring.

2.3. Biometric Technology

The word Biometric[8][14] is gotten from the Greek language it implies BIOMETRICS=BIO-LIFE METRICS-MEASURE (Physical and Behavioral). The infant impressions, alongside a mother's fingerprints, turned out to be a piece of the
clinic's records as a prerequisite by states to help forestall mistakes in medical clinic nurseries. In 1960 and 1970, signature biometric, verification methodology was created. This sprouting utilization of biometrics was then to some degree overlooked, just to be rediscovered by William James Herschel, a British official, to be utilized for a completely extraordinary reason. Having been placed accountable for building streets in Bengal, he had his subcontractors sign agreements with their fingerprints. In 1980 Alphonse Bertillon contemplated body mechanics and estimations to help in recognizing crooks.

3. Digital Watermarking

Digital watermarking[9][19] is an extension of the watermarking concept in the digital world. A digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file’s copyright information (author, rights, etc.).

3.1. Types of Watermarking

Figure 2 Robust and Fragile Watermarking, Visible and Invisible Watermarking, Public and Private Watermarking Asymmetric and Symmetric Watermarking, Steganographic and Non-Steganographic Watermarking.

3.2. Types of Watermarking Scheme

Private (non-blind) watermarking systems require for extraction/detection the original cover-data. Type-I system uses the original cover-data to extract the watermark from stego-data and use original cover – data to determine where the watermark is[9][19].
Type II systems require a copy of the embedded watermark for extraction and just yield a yes/no answer to the question of whether stego-data contains a watermark. Extract using \{D,K,W\}. Semi-private (semi-blind) watermarking does not use the original cover-data for detection but tries to answer the same question. (potential application of blind and semi-blind watermarking is for evidence in court ownership,). Extract using \{K,W\} Public (blind) watermarking- neither cover-data nor embedded watermarks are required for extraction-this are the most challenging problem. Extract using \{K\}. 

Figure 3 Types of Biometric Module. A biometric [17][18] identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioral identifiers. Above diagram says the identifiers is very important three divisions of biometric digital images user must know “something you are”, “something you have”, “something you know” for secured data transmission. These are all divisions are an important role to share authenticated information.

4. Existing Work

As per the less percentage of variations in physical traits in the human body for the biometric digital images are fingerprint and retina[20][22].

Figure 4 Overview diagram of existing work
database and using the Query Based Biometric Database[17][18]. So we should go for image processing concepts that are implemented in java. We created the prototype to conceal the two images like fingerprint and retina masked by using jcap in java[20][22]. To increase the quality of images at the compression technique with the help of DCT[2][3] through MATLAB. Secure authentication with the help of jcap[7][22] covered images through the validation of dynamic key generation. Then validate the end-user and to satisfy the FAR False Acceptance Ratio/FRR False Rejection Ratio [15] [17] of two pictures. For that existing work was biometric framework can be isolated into three phases: The enrollment module, the identification module, The Authentication module. The enrollment module is responsible for training the system to identify a given person. In the identification module, the biometric sensors capture the characteristics of the person. In the authentication module validate the user through these two ratios FAR/FRR.

5. Problem Definition

For existing work, we found the difficulties of a system's FRR [17] [18] typically is stated as the ratio of the number of false recognitions divided by the number of identification attempts. As per the existing concepts to ensure authenticated users through the FAR/FRR ratios [17] system missed the ratio some cases of the attempt the validate the user identification. As the Existing work is done by a combination of MATLAB and JAVA. Finally, the problem definition is my future thesis work during the transmission data lost an in between the communication channels. So we will work out a strongly hidden image through private watermark and ICA[4][5][20][22] technique for secure transmitting the data. MATLAB is a numerical computing environment. As per the performance base, MATLAB is slower than java. So we will go to work out all these concepts through java.

6. Overview of Proposed Work

6.1. Bimodal Biometric Images Using Private Watermarking With IDCT

As the Biometrics images, we will use three digital images fingerprint, retina and photo image. Figure 5 to achieve the watermark we will be taken two text images like Name and DOB. Implementing steganography for secure transmission [1][3] using to conceal and covered the two secret images with the purpose of confidentiality.
In this technology, intruders can’t find a hint about the data during transmissions. Every individual we play a role to increase the level of protection of our datum. So we should go for watermarking techniques. This technique says for the purpose eavesdropper cannot replace or remove the information during the transactions and transmissions. In watermarking, the ICA[20][22] technique is used to attain confidentiality. So that the two original images like fingerprint and retina image wrapped by an authenticated photo image. Then the role of the ICA[4][5][6] technique mixing the two concepts like IDCT [2] [3] and AES on the photo image. Finally extract the two original images with two keys. Through the two keys to transmit the original images both ends sender and receiver.

6.2. Conceal the fingerprint and retina images using steganography technique with private watermarked through authenticated face photo image

Figure 6 is the authentication purpose over the face photo image two NAME & DOB text Images with the help of a private watermark. In that, we use the NAME text image as an invisible watermark and DOB text Image as a visible watermark on the face photo image. Then face photo image converted as watermarked image. The fingerprint and retina original image achieve the stegoanalysis technique through the DCT compression technique. After applied DCT[11][2] on the original image wrapped with a watermarked face photo image for authentication purposes. Here the face photo image converted as a stego image. Then we achieve the ICA[20][22] concepts to mixing technique by IDCT[2][3] and AES[9][19]. Then extract the two keys to retrieve two original images like fingerprint and retina. Here key1 is the DOB text image acted as the visible watermark then key2 is AES encryption algorithm for the hexadecimal format to the sender side. At the receiver side, to extract the two original images like the fingerprint and retina. For that extract, key1 is the DOB text image and the AES decryption algorithm with the hexadecimal format is key2.

![Figure 6. Private Watermarking for face photo image](image)

6.3. Secured steganography technique and implements ICA

Figure 7 The Secured steganography technique and implement ICA. Here we use ICA for mixing two-hybrid techniques like IDCT and AES. Finally, we separate the signal with two keys.
6.4. Fingerprint and Retina images with the face image using DCT and AES

This depicts the representation in Figure 8 explains the compression techniques for DCT[10]. Compare the various compression technique quality-wise DCT is good. Behind the extracted image, at the moment the processing of compression technique with private watermarking scheme de-embedded file. Here this compression ratio shows 102% because the biometrics images resolution quality is high. Then the purpose of secure transmission achieves the encryption technique process will apply on these watermarked images through the AES[10][9][19] algorithm 64 bit. The compatibility and avoid the memory overhead as the dynamic key generation as the hexadecimal format.

Figure 8. De-embedded File Information with Compression details using IDCT technique on GUI environment

Figure 9. Final secret data is a biometric fingerprint and retina covered watermarked face image in a GUI environment.
Finally, the original image fingerprints and retina covered by authenticated private watermarked face photo image with IDCT compression technique [2][3][10] and AES 64 bit encryption algorithm with hexa format.

7. Conclusion and Future Work

In our society privacy is not there now a day. So that privacy is essential to transmitting the datum without aware of crackers. As per the kерchoff’s principle, this prototype is designed very robustly during transmission. We provide security aspects to save our transmitting datum from public sectors like Banking Sectors, CCTV, Social Networks etc., from the crackers. Apart from these cases as per the implementation cost is high nowadays for black chain technology issue we strongly believe 99.55% provide security against crackers or intruders[19]. Even unaware of technology awareness enjoying the technology in a secure way to satisfy the requirements in the future. In this paper, the Co-author contributes section is about cryptography part of the encryption algorithm AES[10]. The paper about our innovation is secure ICA for data transmission. Image processing concept implementation is Java because of the MATLAB mathematical environment. In Future will be implemented as an original image as a node to fix on the NS2 simulator that secret image to transmit in between the sender and receiver. This is the innovation of our future work. When transmitting data within two nodes protect from crackers though the attack Denial of Sleep[11][16]. So that We maintain MAC protocol[11] standards IEEE 802.15.4. This protocol provides the synchronized operation is CSL(Coordinated Sampled Listening)[11] wake-up periodically to scan the wake-up of the channel so-called wake-up the frame. This hint receiver of wake up the frame to temporarily go back to sleep until the transmission of the payload frame is about to begin. These implemented the only defence on the MAC layer.

References

[8] Mandy Douglas, Karen Bailey, Mark Leeney, Kevin Curran. An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools Appl, This article is an open access publication. Published online 29 November 2017. Copyright © Authors 2017. Springer.


