International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Skin Tone Detection Algorithm for an Adaptive DWT Based Approach to Steganography using Biometrics

Mr. Patil Samadhan T.
M.E. Student (Communication Engineering),
SGD College of Engineering Jalgaon
Email: patilsamadhan43@yahoo.com

Dr. Patil A. J.
(Principal) Department of Electronics & Telecommunication
SGD College of Engineering, Jalgaon

***Abstract* – Challenges face biometrics researchers and particularly those who are dealing with skin tone detection include select a colour space, generating the particular skin model and processing the obtained regions. The majority of obtainable methods have in common the de-correlation of luminance from the considered colour channels. Luminance is the miscalculate since it is seen as the least causal colour component to skin colour detection. This type of work questions this claim by showing that luminance can be useful in the segregation of skin and non-skin clusters. To this end, here we use a new colour space which contains error signals derived from differentiate the grayscale map and the non-red encoded grayscale version. The advantages of the approach are the reduction of space dimensionality from 3D, RGB, to 1D space advocating its candor and the construction of a rapid classifier necessary for real time applications. The future method generates a 1D space map without prior knowledge of the host image. A complete experimental test was conducted and initial results are presented. This paper also discusses an application of the method to image steganography where it is used to orient the embedding process since skin information is deemed to be psycho visually redundant**

***Keywords* – Biometrics, Mat Lab, Skin Tone Detection, Stenography.**

I. INTORDUCTION

Biometrics-based stenography attempts to answer the questions “Who are you and “Are you who you claim to be” Personal identification, regardless of method, is ubiquitous in our daily lives. For example, we often have to prove our identity to gain access to a bank account, to enter a protected site, to draw cash from an ATM, to log in to a computer, to claim welfare benefits, to cross national borders, and so on.

The main objective of this project is to provide a highly secured communication between people using the Steganography technique a steganography prefers to hide information as much as possible and requires cover media with distortion as little as possible. The advantage of steganography over cryptography is that messages do not attract attention to attackers and even receivers. For example, hackers often disrupt computer networks; credit card fraud is estimated at $2 billion per year worldwide; and in the USA, welfare fraud (by double dippers) is believed to be in excess of $4 billion a year. In India also different cases are happen like withdrawing of money from other persons ATM, Bank etc.gives motivation to set a powerful biometric system. There are two things that need to be considered while designing the steganographic system: (a) Invisibility: Human eyes cannot distinguish the difference between original and stego image. (b) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly Stenography based on biometrics presents a challenging problem in the field of image analysis and computer vision, and as such has received a great deal of attention over the last few years because of its many applications in various domains. Biometrics is personal physical or biological measurements about an individual. Using biometrics for identifying human beings offers some unique advantages. A biometric based identification system has two modules.
Enrollment module: A user’s biometric data is acquired using a biometric reader and stored in a database. The stored template is labeled with a user identity (e.g., name, identification number etc. to facilitate authentication.

Identification module: A user biometric data is once again acquired and the system uses this to either identify who the user is, or verify the claimed identity of the user. While identification involves comparing the acquired biometric information against templates corresponding to all users in the database, verification involves comparison with only those templates corresponding to the claimed identity. Thus, identification and verification are two distinct problems having their own inherent complexities. The unique features of biometric traits are extracted either from spatial domain or transform domain.

(a) Spatial domain techniques viz., Principal Component Analysis (PCA), Independent Component Analysis (ICA),Linear Discriminative Analysis (LDA) ,Singular Value Decomposition(SVD)

(b) Transform domain techniques where in the biometric data from spatial domain is converted to transform domain viz., Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Dual Tree Complex Wavelet Transform (DTCWT) etc. The features of the test image are compared with the data base images in matching section to identify a person using (i) Euclidean Distance (ED),(ii) Hamming Distance (HD),(iii) Support Vector Machine (SVM), (iv) City Block Distance(v) Neural Networks (NN) etc.

II. LITERATURE SURVEY

Today major part of communication goes through internet and this communication needs to be secret and protected against malicious attacks. Steganography is the art and science of invisible communication. It not only keeps the contents of a message secret, but also the existence of message secret. There exist many different steganography technique having different strong and weak points.

International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

2.1 Chaffing and Winnowing:

Chaffing and winnowing is a cryptographic technique to achieve confidentiality without using encryption when sending data over an insecure channel; it was conceived by Ron Rivest It can be viewed as a form of steganography. The sender (Alice) sends several messages to the receiver (Bob); each message is unencrypted but authenticated with a message authentication code(MAC) whose secret key Alice shares with Bob. Only one of the messages is authentic, the other ones are bogus (called "chaff"). An eavesdropper will be unable to tell which messages are bogus and which are real (i.e. to "separate the grain from the chaff") since he cannot determine which messages are authentic. Bob uses the MAC to find the authentic messages and drops the "chaff" messages. This process is called "winnowing".

2.2 Invisible Inks

Invisible ink is a substance used for writing, which is either invisible on application, or soon thereafter, and which later on can be made visible by some means. The use of invisible ink is a form of Steganography, and has been used in espionage. Invisible ink is applied to a writing surface with a fountain pen, toothpick or even a finger Dipped in the liquid. Once dry, the paper should appear blank or the ink is not an invisible Ink. The ink is later developed (made visible) by different methods according to the type of invisible ink used. This can be by heat, by viewing under ultraviolet light, or by applying a chemical appropriate for the ink used.

2.3 Null Cipher

A null cipher is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. It would today be regarded as a simple form of steganography. Null ciphers can also be used to hide cipher text, as part of a more complex system. In classical cryptography a null is intended to confuse the cryptanalyst. Typically, a null will be a character which decrypts to obvious nonsense at the end of an otherwise intelligible phrase. In a null cipher, most of the characters may be nulls.

III. BLOCK DIAGRAM

Fig.1 gives overview of stenographic system with the basic steps involved .This section describes different techniques with its types, advantages and disadvantages to give clear idea about specific techniques which have been selected for proposed stenographic system like selection of cropping part from whole image ,selection of which wavelet transform ,techniques for feature extraction etc.

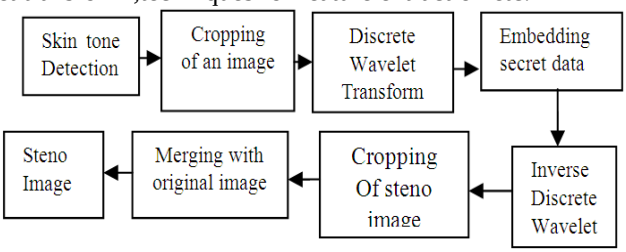

Fig.1. Block diagram of stenographic skin tone detection system

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word *steganography* is of Greek origin and means "concealed writing" from the Greek words *steganos* (στεγανός) meaning "covered or protected", and *graphei* (γραφή) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.
The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it. Steganography is a technique to hide secret messages in a host media called cover media. The advantage of steganography over cryptography is that messages do not attract attention to attackers and even receivers. Steganography and cryptography are often used together to ensure security of the secret messages. For example, many previous steganography approaches use the secret key (i.e., idea borrowed from cryptography) to produce better protection of the information if the stego object arouses suspicion. Therefore, these approaches can become more secure and can be potentially useful to some security-demanding applications such as military intelligence. Watermarking is another popular technique to hide messages and it is usually used for providing ownership on copyrighted multimedia material and for detecting originators of illegally made copies. Therefore, an effective watermarking method must be robust against a variety of attacks. In contrast to watermarking, steganography prefers to hide information as much as possible and requires cover media with distortion as little as possible. The main objective of this project is to provide a highly secured communication between people using the Steganography technique a steganography prefers to hide information as much as possible and requires cover media with distortion as little as possible. The advantage of steganography over cryptography is that messages do not attract attention to attackers and even receivers. Today major part of communication goes through

internet and this communication needs to be secret and protected against malicious attacks. Steganography is the art and science of invisible communication. It not only keeps the contents of a message secret, but also the existence of message secret. There exist many different steganography technique having different strong and weak points. In this paper steganography is based on biometric feature i.e. secret data is embedded in skin tone regions of an image. Secret data is hidden by tracing skin pixels

In one of the high frequency sub band of DWT of the cover image To enhance the high security feature secret images are dispersed within each band using a pseudo random sequence and a session key. This combined approach of using skin pixels and spread spectrum for embedding the secret images provides a high degree of security. The stego image generated is of acceptable level of imperceptibility and distortion compared to the cover image.Steganographyis a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to Cryptography, where the existence of the message itself is not disguised, but the meaning is obscured. "Steganography" is a Greek word and means 'covered or hidden writing'. Its origins can be traced back to 440 BC. Steganography has been widely used in historical times, especially before crypto graphical systems were developed. Examples of historical usage include:

• Hidden messages in Wax tablets: In ancient Greece, people wrote messages on the wood, and then covered it with wax so that it looked like an ordinary, unused, tablet.
Hidden messages on messenger's body: Also in ancient Greece. Herodotus tells the story of a message tattooed on a slave's shaved head, covered by hair re growth, and exposed by resaving. The message, if the story is true, carried a warning to Greece about Persian invasion plans. Hidden messages on paper written in secure inks under other messages or on the blank parts of other messages.

During and after World War II, Espionage agents used microdots to send information back and forth. Since the dots were typically extremely small -- the size of a period produced by a Typewriter (perhaps in a font with 10 or 12 characters per inch) or even smaller --the stegotext was whatever the dot was hidden within. If a letter or an address, it was some alphabetic characters. If under a postage stamp, it was the presence of the stamp.

The one-time pad is a theoretically unbreakable cipher that produces cipher texts in distinguishable from random texts: only those who have the private key can distinguish these cipher texts from any

Other perfectly random texts. Thus, any perfectly random data can be used as a covertext for a theoretically unbreakable steganography.

IV. Conclusion & Future Scope

One approach to increase accuracy and reduce training time is combining multiple independent feature sets of stenography and cryptography, where the weakness of one method is compensated by the strength of another, may improve the skin tone detection of individual person. Throughout this project we have only focused on the security problem. We subsequently developed methods which enable us to determine if the processing like DWT can be advanced by multiple levels and different transforms. For instance, instead of seeking to determine the identity of an individual our main aim to distinguish some other feature. Possible suggestions include: gender; hairstyle; the presence of eye glasses or even facial expression. The frontiers of research within have now moved towards the recognition of cursive script that is handwritten connected or calligraphic characters. Promising techniques within this area, deal with the authentication of person based on lip movement tracking. With the help of DSP processor we can speed up the process of face detection and face recognition techniques. We can implement this technique in real time application. We can also implement this technique with hardware.

References

[1] Paul Nicholl, Abbes Amira, Djamel Bouchaffra, "Multiresolution Hybrid Approaches for Automated Face Recognition", Proceedings of the IEEE 2nd NASA/ESA Conference, Edinburgh.pp.89-96, 5-8 August 2007

[2] Principle Component Analysis, Eigen face and Neural Network, "Signal Acquisition and Processing, IEEE International Conference on, pp. 310-314, 2010

[3] Janarthany Nagendrarajah , "Recognition of Expression Variant Faces – APrinciple Component Analysis Based Approach for Access Control", IEEE, 978-1-4244-6943-7, 2010

[3] W.Zhao, R.Chellappa, P. J. Phillips, A. Rosenfeld, "Face Recognition: A Literature Survey", ACM Computing Surveys, Vol. 35, No. 4, pp. 399–458 December 2003,

[4] M.Turk, A.Pentland,"Eigenfaces for Recognition", Journal of Cognitive Neurosicence, Vol. 3, No. 1, pp. 71-86 ,year 1991

[5] W. Zhao, R.Chellappa, A. Krishnaswamy, "Discriminant Analysis of Principal Components for Face Recognition", Proceedings of the 3rd IEEE International Conference on face and Gesture Recognition, FG" 98, 14-16 pp.336-341 April 1998

[6] P. N. Belhumeur, J. P. Hespanha, and D.J. Kriegman "Eigen faces vs. Fisher faces: Recognition using Class Specific Linear Projection", IEEE Transaction on Pattern Analysis Machine Intelligence (PAMI), Vol.19, pp., 711–720.year 1997

[7] T .Kanade, "Computer recognition of human faces", Birkhauser, Basel, Switzerland, and Stuttgart, Germany, 1977

[8] L.I.Smith, "A tutorial on Principal Components Analysis".

[9] L. Wiskott, J.M. Fellous, N. Kruger, C. Malsburg, " Face Recognition by Elastic Bunch Graph Matching", IEEE Transaction on Pattern Analysis Machine Intelligence (PAMI), Vol.19, pp. 775–779 ,year 1997

[10] J. Huang, B. Heisele, V. Blanz, "Component-based Face Recognition with 3D Morphable Models", Proceedings of the 4th International Conference on Audio and Video Based Biometric Person Authentication (AVBPA), pp. 27-34 ,09-11 June 2003

[12] Bouckaert, Frank, M. Hall, R.kirkby, P. Reutemann, A. Seewald, D. Scuse, "*WEKA Manual for Version 3-6-2", Ch* no 4.3 P.no.41, January 11, 2010

[13] Data Mining Practical Machine Learning Tools and Techniques, Second Edition By Ian H. Witten and Eibe Frank

AUTHOR'S PROFILE

Mr. Patil Samadhan T.

I was born on 12th may 1987 at bambrud raniche tal-pachora dist-jalgaon. I have completed my degree BE(E&TC) from the SNJB COE chandwad dist-Nasik in 2009.after that I have taken admission for post graduated course ME (Communication) from shri gulabrao college of engineering jalgaon.
Mr. Patil S.T was life time member of ISTE.

Dr. Patil A. J.

(Principal) Department of Electronics & Telecom-munication
This paper is published under the guidance of Dr. A. J. PATIL
He is working as principal at SGD COE JALGAON.
Email: principal@coe jalgaon