International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

Resourceful and protected Biometric Image Stenography using Discrete Wavelet Transform

PATIL S.T M.E. (Communication), North Maharashtra University SGD College of Engineering Jalgaon

Dr. Patil A.J (PRINCIPAL) Department of E&TC SGD College of Engineering, Jalgaon

Prof.Patil C.S H.O.D E&TC SGD College of Engineering, Jalgaon

Abstract— Steganography is the science of concealing the existence of data in another transmission intermediate It does not return cryptography but rather boosts the security using its gloom features. As proposed method is Biometric Steganography, here the Biometric feature used to implement Steganography is Skin tone region of images. Proposed method introduces a new method of embedding covert data within the skin portion of the image of a person, as it is not that much receptive to HVS (Human Visual System). in its place of embedding secret data anywhere in image, it will be embedded in only skin tone region. This skin region provide superb secure location for data hiding. So, firstly skin detection is performed in cover images and then Secret data embedding will be performed in DWT domain as DWT gives better performance than DCT while compression. This biometric method of Steganography enhances robustness than existing methods.

Keywords—Biometrics, Matlab, Skin Tone Detection, IDWT, Cropping PSNR, RGB Panel, MSE

I. INTRODUCTION

Steganography differ from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the life of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly overcome. The strength of stenography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the logical property owner to identify customers who break their licensing agreement by supplying the property to third party In steganography secret data is the data that the sender wishes to send to the receiver. It can be audio, video, image, text file, or other data. They is represented as the stream of bits. This secret data is hidden on the medium or cover or host. Medium of communication is also the image. In this paper secret data is restricted to digital images. Cover image with secret data embedded is called Stego-Image.

II. LITERATURE SURVEY

Instead of embedding data anywhere in the image secret data is needed to be embedded in the skin region of the image. For that input image is converted into an appropriate color space [1].Mainly two kinds of color spaces are suitable for biometric operations. HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces. For the skin color tone detection [7] a skin detector and a skin classifier was there. Skin detector converts the cover image of RGB color space into appropriate color space. Skin classifier will classify pixels in the cover image to skin and non skin pixels by defining a boundary. The skin detection algorithm produces a mask, which is simply a black and white image. The black pixel values are 0 (false) and the white pixel values are 1 (true). For this paper HSV color space is choose. For that first, the image in RGB was converted to HSV color space, because it is more related to human color perception. Hue-saturation based color spaces were introduced when there was a need for the user to specify color properties numerically. In HSV, responsible vales for skin detection are Hue & Saturation so extract the Hue and Saturation dimensions into separate new variables (H & S). For skin detection threshold should be chosen as [H1, S1] & [H2, S2]. A pixel is classified as skin pixel if the values [H, S] fall within the threshold. Threshold is predefined range associated with the target skin pixel values. Most of the researchers determined threshold as h_range = [0, 0.11] and s_range = [0.2, 0.7].

Fig 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. 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 steganographyis 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 1499by Johannes Trithemius in his Steganographia, a treatiseon cryptography and steganography disguised as a bookon magic.
Generally, messages will appear to be something else: images, articles, shopping lists, or some othercover text and, classically, the hidden message may be ininvisible ink between the visible lines of a private letter.The advantage of steganography over cryptography aloneis that messages do not attract attention to themselves

III BLOCK DIAGRAM

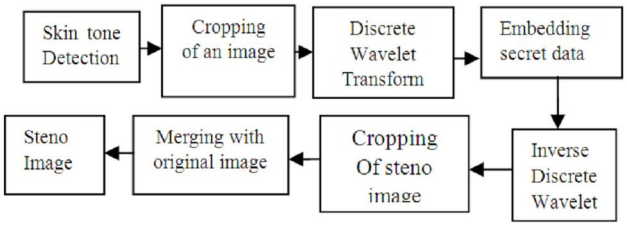

Fig. skin tone detection

.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. can extract message without having value of cropped region. 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 pseudorandom 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. Steganography is 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 to440 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 one 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 12characters per inch) or even smaller --the stego text was whatever the dot was hidden within. If a letter or an address, it was some alphabetic characters. If under 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 cover text for a theoretically unbreakable steganography.

IV. RESULTS

Image Type	Image Resolution	DWT levels (Haar Transform) After resizing(256x256)
2.jpg	320x400	LL =65x65
		LL1=33x33
		LL2=17x17

Image Type	Image Resolution	DWT levels	MSE	PSNR
2.jpg	320x400 (after resizing 256x256)	DWT1 (Haar)	0.0053	70.39
		DWT1db	0.0041	71.53
		DWT1db5	0.0041	71.98
		DWT1db7	0.0043	71.83

V. CONCLUSION & FUTURE SCOPE

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. In this paper biometric steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced, maintains security at respectable level since no one can extract message without having value of cropped region. Features obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. According to simulation results, proposed approach provides fine image quality.

According to results I have concluded that for DWT level1 with Haar transform gives better extraction results compare to daubeshian wavelets which decrasws certain amount of extraction coefficients' which affects extracted logo image. As well as optimized level of daubeshian is db5 after trail and error because for db7 psnr value will change.

REFERENCES

[1] Simon ClippingdaleMahitoFujii "Skin Region Extraction andPerson- independent" NHK (Japan Broadcasting Corporation),Science & Technology Research Labs IEEE 2011.

[2] Anjali A. Shejul Prof. U.L Kulkarni "A DWT baseApproachfor Steganography Using Biometrics" International Conferenceon Data Storages &Data engg,IEEE 2010.

[3] Johnson, N. F. and Jajodia, S.: Exploring Steganography:Seeing the Unseen. IEEE Computer, 31 (2): 26-34, Feb 1998.

[4] Johnson, N. F. and Jajodia, S.: "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.

[5] Fridrich, J., Goljan, M. and Du, R.., (2001). "Reliable Detection of LSB Steganography in Grayscale and Color Images." Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.

[6] Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290.

