USE OF RANDOM PIXEL SELECTION AND 7-BIT REPRESENTATIONS TO INCREASE THE CAPACITY AND SECURITY OF SKIN TONE IMAGE STEGANOGRAPHY

Sonali Powar*
Assistant Professor, Department of Computer Sciences, Vishwakarma University, Pune, India.

Ishita Dixit
Assistant Professor, Department of Computer Sciences, Vishwakarma University, Pune, India.

Jupinder Kaur
Assistant Professor, Department of Engineering Sciences, Vishwakarma University, Pune, India.
***Corresponding author E-mail id: sonali.k.powar@gmail.com**

Abstract
A vast volume of information is transferred over the internet in the digital era, posing a security and authenticity challenge. To get over the security problem, undetectable data concealing is used. Steganography conceals the existence of sensitive information. This paper describes an approach that is secure and has good data hiding capacity. The approach hides text information inthe cover image's skin tone area. The skin tone detector algorithm detects the skin tone area, which is subsequently cropped before the secret information is hidden. To boost payload, 7-bits are employed to represent text data. The skin tone area of the cover image is transferred into the frequency domain using integer wavelet transformation (IWT). The embedding method utilizes the blue channel's HH, HL, and HH sub-bands and even the green channel's HH sub-bands. The IWT coefficient is chosen using a random generator, which promotes security, and the 2K correction is applied to reduce distortion. The PNSR results obtained with this method are acceptable.

Keywords: image steganography, IWT, 2k correction, random pixel selection, skin tone steganography

1. INTRODUCTION

The technique of hiding data into another carrier medium is called as steganogrphy. Good steganography providesa large capacity with less imperceptibility. In ancient Greek used wax tables hide the message

"The person would scrape the wax off a tablet, write a secret message on the underlying wood andagain cover the tablet with wax to make it appear black or unused" (Johnson, N. and Jajodia, S., 1998). Another technique involved shaving the massager's head and tattooing a hidden message on it. After the hair regrows, a massager is sent to the location where the head is shaved to reveal the secret message. People used invisible ink for writing secret messages during the initial period of the World War II. They also used invisible for writing secret messages between lines of the innocent letter. Secret data was also hidden in the document itself. A clear message was written in the document, but confidential data was present. By extracting specific position letters, data would be retrieved. To conceal data in digital steganography, many carrier mediums such as text, image, audio, and videoare used. The use of an image as a carrier medium is termed as image steganography. Many technologies such as spatial domain, frequency domain, spread spectrum, masking filtering, distortion, etc., are used to embed data in images (Patil et al., 2020).

Figure 1 shows the different techniques used to hide data in the image. The spatial domain providesgood capacity but it is a less secure method. The most popular spatial domain method is LSB. In this method, the least significant bit of pixels are used for embedding the data. We can enhance capacity by increasing thenumber of message bits per pixel, but visual distortion also increases. In the case of the frequency domain, different transformations like DCT, DWT, DFT, IWT etc. are used for transforming the cover image from the spatial domain to the frequency domain (Kharade et al., 2019).

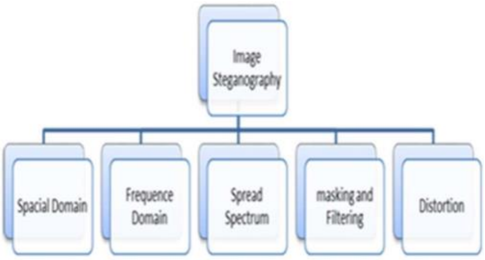

Figure 1: Image steganography Techniques

The frequency-domain technique has less embedding capability but is more robust than the spatial domain approach. Data is hidden in a specific region rather than the entire image to increase security. This sort of steganography is known as region-based or object-based steganography. Skin tone steganography is region-based steganography in which data is only embedded in the skin tone area.
The spread spectrum image steganography concept is "spreading bandwidth of narrow signal across a wide band of frequencies" (Subhedar, M. and Mankar, V., 2014). Marvel et al has invented the spread spectrum image steganography. It is difficult to detect a narrow band signal after being spread across a wide frequency band. The resulting signal is embedded into the cover image to obtain the stego image. Because the power of the cover image is significantly greater than
the power of the embedded signal, the SNR (signal to noise ratio) is low. When the SNR is low, it indicates that the perceptibility is low. A good synchronization of the pseudo-random noise generators at both the transmitter and the receiver is required. Otherwise, the desired results will not be obtained (Subhedar, M. and Mankar, V., 2014). The sender and receiver use same key (symmetric key) to the encoding and decoding process. This method resists additional noise and compression also.
The masking and filtering technique is similar to watermarking. It creates marks in the cover image. In this technique, it is hidden into more significant areas instead of hiding data in noise level. This technique does not change image visual properties so that image change should not benoticed with the naked eye (Masoud Nosrati, et al. 2011). The advantage of this method is, more robust against compression than LSB method as data is hidden invisible parts of an image. The disadvantage is this technique is mainly applied only on gray scale or 24-bit images (Pratap Chandra Mandal, 2012).
The distortion technique is un-blind image steganography. It means to extract secret messages we require cover image and stego image. The decoding function checks the difference between the cover and stego image to extract secret messages. "Encoder adds a sequence of change to cover image. So, information is described as being stored by signal distortion" (H.S. Majunatha Reddy and K.B. Raja. 2009). The stego image is obtained by application of a sequence of modifications in the cover image. While encoding processes, the pixel is chosen randomly. The limitation of this technique is that we have to send a cover image and stego image.
(Po-Yueh Chen and Hung-Ju Lin 2006) Proposed a method in which DWT transformation is usedand low-frequency sub-band LL is kept untouched to maintain image quality. Data is embedded in two modes fixed (fixed bits per pixel) or variable. While embedding, a key matrix is generated which is also embedded in the image. Data cannot be extracted without the key matrix. This method gives good PSNR values for higher capacity.
(Shejul and Kulkarni, 2011) use skin tone region to hide data. HVS colour space is used to detectskin tone area. The cover image is transferred into the frequency domain by using DWT. The skin pixel's

DWT coefficient contains secret data hidden in one of the high-frequency sub-bands of the DWT coefficient. Their study looked at both cropping and non-cropping methods and concluded that cropping provides more security while non-cropping preserves histogram. This method produces images with excellent quality (Shejul, A. and Kulkarni, U. 2011).

(Behbahani, Ghayour and Farzaneh, 2011) Proposed a method in which an 8X8 DCT quantized block is divided into 2X2 sub-blocks. Each submatrix has an eigenvalue and eigenvector. By changing these attributes, secret data is embedded in DCT coefficient of image. This method provides resistance against subtractive pixel adjacency matrix (SPAM) but it provides low payload capacity (Khodaei and Faez, 2012) proposed a method based on LSB substitution and PVD. This technique partitions the cover image into 1x3 non-overlapping blocks. Using the optimal bit substitution method, K-bits are stored into the central pixel called the base pixel. The difference between the new value of base pixel and the value of other two pixels is used to calculate the number of bits that can be stored into the other two pixels (Khodaei, M. and Faez, K. 2012).

(Prabakaran G. et al. 2014) uses IWT as well as DWT transformation so-called as dual wavelet transformation. This technique provides high capacity and security and also increases performance. Dual transformation is applied on secret images, hidden using the fusion technique.The secret image is hidden in any one channel Red, Blue or green. This method achieves good image quality (Prabakaran G et al. 2014).

(M. Kude and M. Borse 2016) uses HVS color space to find skin tone area. The secret image is hidden in blue panel of skin tone area. Before hiding, the cover image is converted into a frequency domain using Haar-DWT. Only LL sub-band of the secret image is used for the embedding process. This method works with any type of image format. This method gives better PNSR and MSE values (Manisha Kude et al. 2016).

(Muhammad et al., 2016) proposed a method called CISSKA-LSB. This method encrypts the stego key using the two-level encryption algorithm (TLEA), and embeds the secret data using the multi-level encryption algorithm in this method (MLEA). It is used in this method to indicate which channel contains data using a single channel that serves as an indicator. As a result, payload capacity is reduced because only one channel is used to embed data (Muhammad et al., 2016).

(K and Vas P, 2018) detects skin area using YCbCr colour space. Instead of hiding datasequentially, the pixels are randomly selected using a pseudo-random generator. The data is hidden in LSB bit of randomly selected pixel. This method provides good PNSR value i.e. good image quality. Also, the MSE value calculated using this method is less. So this method is more robust (K, A. and Vas P, S. 2018).

2. RELATED WORK

2.1 SKIN TONE DETECTION

Instead of hiding data in the whole image, the skin tone area of the image is used to hide data. If data is embedded into skin tone area it is not much sensitive to the human visual system (A. Cheddad et al. 2008). In the proposed method, HVS and YCbCr color space is used. The pixels whose range of Cr is 140 to 165, the range of Cb is 140 to 195, and the range of hue is 0.01 to 0.1are treated as skin pixels and non-skin pixels otherwise.

Following equations are used to find cb and cr values of RGB image

cb = 0.148* I(:,:,1) - 0.291* I(:,:,2) + 0.439 * I(:,:,3) + 128;(2.1)

cr = 0.439 * I(:,:,1) - 0.368 * I(:,:,2) -0.071 * I(:,:,3) + 128;(2.2)

In above equation I is RGB image. I(:,:,1) represents Red panel, I(:,:,2) represents Green panel and I(:,:,3) represents Blue panel.

Following MATLAB function is used to convert RGB image into HVSimg_hvs=rgb2hsv(img_org);

2.2 CROPPING

Skin tone area is cropped before applying IWT. Cropping provides more security (Swapnali R et al.) as without a secret key no one can extract secret data (Shejul et al.. 2011). The area which contains a large amount of skin pixels is cropped.

2.3 INTEGER WAVELET TRANSFORMATION

IWT is a lossless transformation technique. In this technique, the original image is reconstructed again without distortion when reverse transformation is applied. This cannot be achieved using DWT or DCT. In DCT, the image is divided into 8X8 pixel blocks and the DCT is applied on each8X8 block. In case of IWT, the transformation is applied on the whole image at a time. In DWT, we get float value, whereas in IWT we get integer values. "Hiding data in integer coefficient provides high imperceptibility and increases robustness" (Raftari, N., 2012). When IWT is appliedon an image four sub-bands are created LL, LH, HL, HH respectively (Rima V G et al. 2019).

Figure 2 shows filtering used in wavelet transformation which divides the image into two parts. Further, these two parts are passed vertically from low and high pass filters (column wise). This produces the following four parts:

a) LL (Horizontally and Vertically Low Pass),
b) LH (Horizontally Low Pass and Vertically High Pass)
c) HL (Horizontally High Pass and Vertically Low Pass)
d) HH (Horizontally and Vertically High Pass).

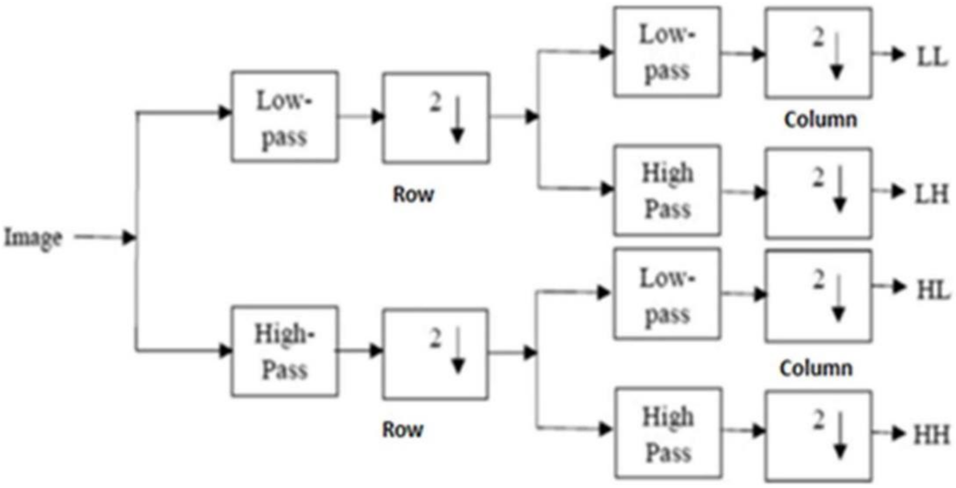

Figure 2 - Filtering used in wavelet transformation

In the proposed method, skin tone area is used to hide secret data. The red channel contributesmore in skin tone area so it is not used embedding process. So, IWT is applied only on blue and green channels.

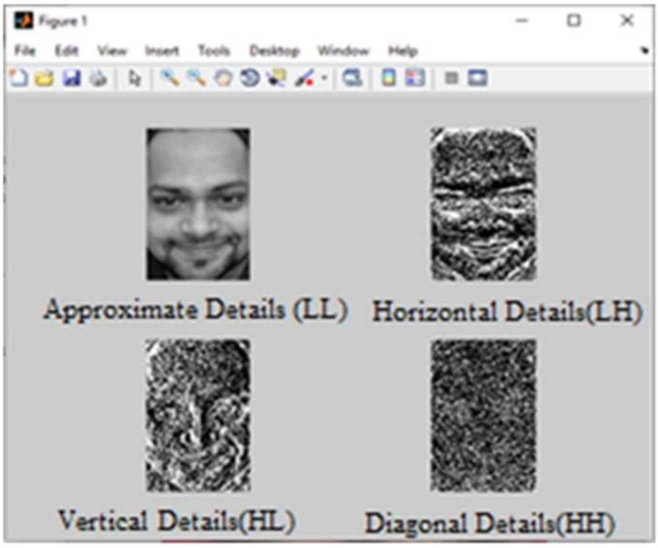

Figure 3 – LL, LH, HL, HH Sub-bands of blue channel

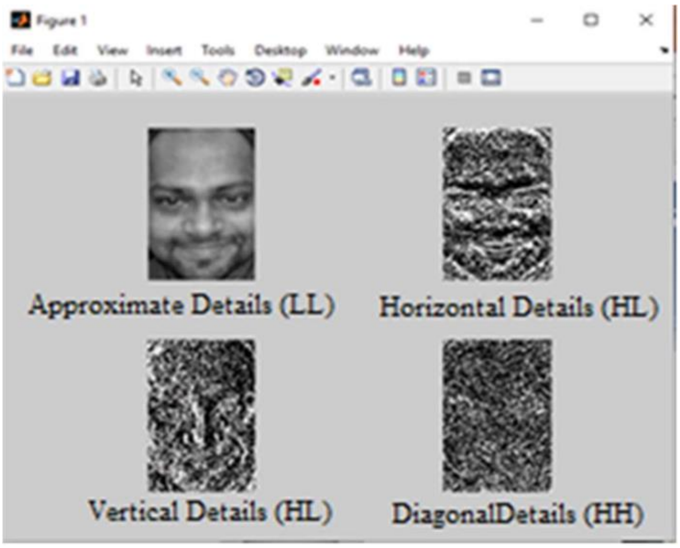

Figure 4 – LL, LH, HL, HH Sub-bands of green channel

Figure 3 and figure 4 shows the LL, LH, HL and HH Sub-bands of blue and green channel. LL sub-band is an approximate sub-band that carries more information about the image. So, changesmade in LL sub-band cause more distortion in original image. The proposed method uses HH, HLof blue and HH sub-band of green channel to carry secret information.

2.4 SECRET TEXT PROCESSING

The proposed method hides text into the cover image. Table 1 shows the characters whose ascii value is in between 1 and 127. The most commonly used characters have ASCII values between 1and 127. So, only 7-bits are sufficient to represent these letters. This method uses 7-bit representation for characters whose ASCII value is less than 127. The 8-bits are only used for characters whose ASCII value is in between 128 and 255. So, this method works for all characters whose ASCII value is between 1 and 255. This concept increases embedding capacity to some extent. Table 1 shows characters whose ASCII value is between 1 and 127 with 8-bit representation. In this case, the leftmost bit is '0'. So, there is no need to embed it into the coverimage (Kharade et al., 2019).

Table 1. Character ASCII (1 to 127) value table.

Dec	Binary	Char	Dec	Binary	Char	Dec	Binary	Char	Dec	Binary	Char
0	00000000	NUL	32	00100000	space	64	01000000	@	96	01100000	`
1	00000001	SOH	33	00100001	!	65	01000001	A	97	01100001	A
2	00000010	STX	34	00100010	"	66	01000010	B	98	01100010	B
3	00000011	ETX	35	00100011	#	67	01000011	C	99	01100011	C
4	00000100	EOT	36	00100100	$	68	01000100	D	100	01100100	D
5	00000101	ENQ	37	00100101	%	69	01000101	E	101	01100101	E
6	00000110	ACK	38	00100110	&	70	01000110	F	102	01100110	F
7	00000111	BEL	39	00100111	'	71	01000111	G	103	01100111	G
8	00001000	BS	40	00101000	(	72	01001000	H	104	01101000	H
9	00001001	HT	41	00101001	)	73	01001001	I	105	01101001	I
10	00001010	LF	42	00101010	*	74	01001010	J	106	01101010	J
11	00001011	VT	43	00101011	+	75	01001011	K	107	01101011	K
12	00001100	FF	44	00101100	,	76	01001100	L	108	01101100	L
13	00001101	CR	45	00101101	-	77	01001101	M	109	01101101	M
14	00001110	SO	46	00101110	.	78	01001110	N	110	01101110	N
15	00001111	SI	47	00101111	/	79	01001111	O	111	01101111	O
16	00010000	DLE	48	00110000	0	80	01010000	P	112	01110000	P
17	00010001	DC1	49	00110001	1	81	01010001	Q	113	01110001	Q
18	00010010	DC2	50	00110010	2	82	01010010	R	114	01110010	R
19	00010011	DC3	51	00110011	3	83	01010011	S	115	01110011	S
20	00010100	DC4	52	00110100	4	84	01010100	T	116	01110100	T
21	00010101	NAK	53	00110101	5	85	01010101	U	117	01110101	U
22	00010110	SYN	54	00110110	6	86	01010110	V	118	01110110	V
23	00010111	ETB	55	00110111	7	87	01010111	W	119	01110111	W
24	00011000	CAN	56	00111000	8	88	01011000	X	120	01111000	X
25	00011001	EM	57	00111001	9	89	01011001	Y	121	01111001	Y
26	00011010	SUB	58	00111010	:	90	01011010	Z	122	01111010	Z
27	00011011	ESC	59	00111011	;	91	01011011	[	123	01111011	{
28	00011100	FS	60	00111100	<	92	01011100	\	124	01111100	|
29	00011101	GS	61	00111101	=	93	01011101	]	125	01111101	}
30	00011110	RS	62	00111110	>	94	01011110	^	126	01111110	~
31	00011111	US	63	00111111	?	95	01011111	_	127	01111111	DEL

2.5 The 2k Correction

In the proposed method 3 least significant bits (LSB) are used to hide data. In 2Kcorrection, k means the number of bits used in data hiding process. "2k correction provides bette imperceptibility" (Yu, J., Yoon, et al. 2008). After hiding data in 3 least significant bits of IWT coefficient, 2k correction is used to reduce the difference between old and new coefficient value. This difference is called error. In the proposed method value of k is 3 as 3 bits are used to hide data. So Possible range of error is

-(2k -1) < = error <= (2k -1)
i.e. -7 to +7 as the value of k is 3.
If the difference is greater than 2k-1 then 2k correction is applied to reduce error. In the proposed method, if the error is greater than 4(as k=3 so 23-1=4) then 8 (as k=3 so 23=8)is subtracted fromthe new IWT coefficient value. If an error is negative, add 8 into the new IWT coefficient.

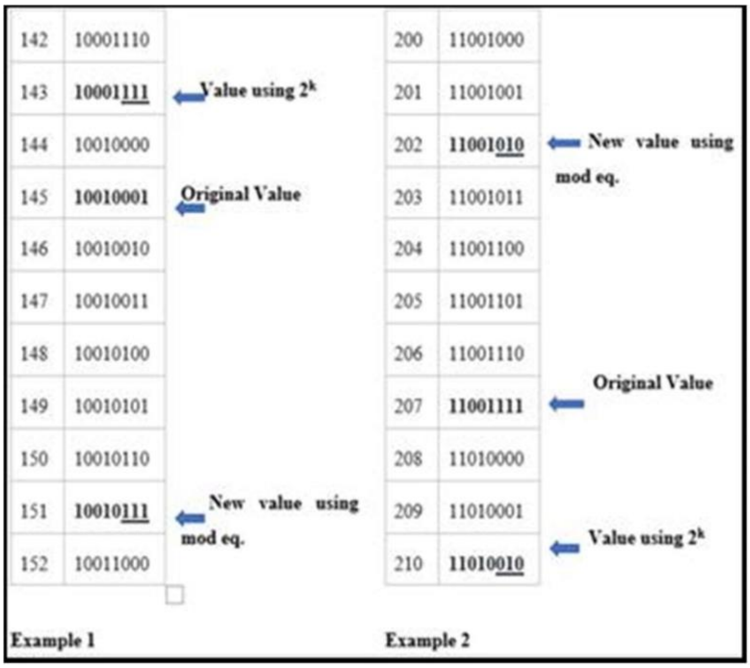

Figure 5: working of 2k correction method

Figure 5 shows the working of 2k correction method. In first example, the original value of IWT coefficient is 10010001(145 in decimal) and after hiding secret data 111 it becomes 10010111(151in decimal). So, in the first example, the difference between the old and new coefficient values is6 (151-145). The 2k correction method is applied to reduce this difference. In the first example, the difference is positive so 8 is subtracted from new coefficient and the resultant value is 1001111(143 in decimal). After appling 2k correction the difference becomes 2(145-143). The original value is 11001111(i.e. 207) in the second example. After hiding data 010, the resultant value is 11001010 (202). In the case of the second example, the difference is -5 (202-207) so to reduce this, the 8 value is added into the new coefficient to get an updated coefficient value. The updatedcoefficient value is 11010010(i.e. 210) and the new difference becomes 3 only (210-207).

3. PROPOSED METHOD

This method uses IWT (Integer Wavelet Transformation) to transfer an image from the spatial domain to the frequency domain. Before embedding data, some operations are applied on the coverimage like preprocessing, skin tone detection, cropping and transformation. At the end, random pixel sequence is generated to embed data.

3.1 EMBEDDING PROCESS

The skin tone area of the cover image is detected, cropped, and preprocessed to avoid overflow and underflow problems. IWT is applied on blue and green channels of the cropped area. The HHand HL sub-bands of the blue channel and only HH sub-band of the green channel is used to embed secret information. IWT coefficients are randomly selected, 3 secret bits are embedded into 3 rightmost bits of the selected IWT coefficient, and 2k correction is applied to reduce the difference(Kharade et al.,

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

2020).
Algorithm to Embed data in the skin tone area of the cover image:
Input: Cover image, secret text messageOutput: Stego image, Secret key
Step 1: Select cover image C and the secret data file.
Step 2: Detect skin tone in cover image C using a skin tone detection algorithm.
Step 3: Crop rectangle area from cover image C, containing the maximum number of skin pixels. Step 4: Extract the blue and green channels of cropped area and apply IWT transformation to get IWT coefficients. Use HH, HL sub-band coefficients of blue channel and HH sub-band coefficients of the green channel.
Step 5: Create a binary stream of secret data using 7-bit representation for characters whose ASCIIvalue is less than 128 and 8-bit representation for characters whose ASCII value is greater than 127.
Step 6: If the length of secret text > payload of the cover image, then go to 13 Else go to 7
Step 7: Sequentially select three bits 'x' from the secret binary stream and randomly select IWT coefficient 'IC'.
Step 8: Hide selected bits 'x' into selected 'IC' using equation IC' = IC – IC mod 2k + x. Apply 2k correction to reduce distortion.
Step 9: If secret data is over then go to Step 10 Else go to step 7
Step 10: Apply inverse IWT on blue and green channel and combine Red, updated Green and updated blue channel to get updated cropped RGB image.
Step 11: Merge updated cropped area with cover image C to get final stego image.
Step 12: Generate secret key using position of cropped rectangle in cover image and length of message.
Step 13: Stop.

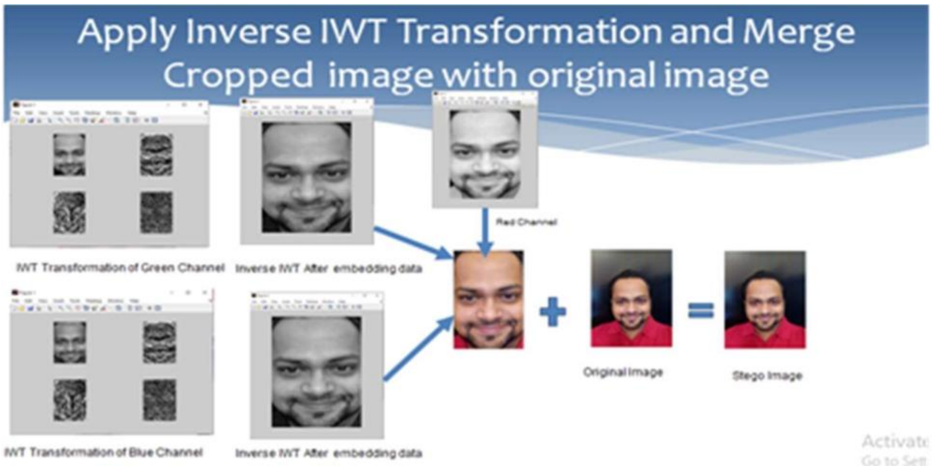

Figure 6 – Process of Embedding data in skin tone area of cover image:

Figure 6 shows the process of hiding data into skin area using proposed method. The data is hiddeninto HL and HH sub band of blue channel and HH sub band of green channel. After completion of data hiding process, inverse IWT is applied on blue and green channels. The updated blue and green channel is combined with the red channel to get a cropped RGB image containing confidential data. Lastly cropped image is merged with the original image to get stego image.

3.2 EXTRACTION PROCESS

A secret key is required to extract secret data from stego image. The length of secret data is calculated using secret key and skin tone area is also cropped using secret key. Then IWT is applied on blue and green channels of the cropped area. Finally, the bitstream is created by extracting last 3 bits of the randomly selected IWT coefficient. After extracting all secret bits, divide the bitstream into 7 bits for characters having ASCII value less than 128 and divide into 8 bits whose ASCII value is greater than equal to 128. Convert all 7 bits and 8 bits blocks into ASCII value and then find their respective character. Finally, write all the characters in the file secret.txt and display filesecret.txt.

Algorithm to extract data from Stego imageInput: Stego image, secret key
Output: secret text messageStep 1: Select stego image.
Step 2: Using secret key, crop the rectangle area from stego image. Also, calculate the length of secret text.
Step 3: Extract blue and green channels from the cropped area and apply IWT on it to get IWT coefficients.
Step 4: Use IWT coefficients of HH, HL sub-bands of blue channel and HH sub-band of green channel.
Step 5: Generate same random sequence of IWT coefficient like sender using rng() and randperm() MATLAB function.
Step 6: Set binary stream B='' or blank.
Step 7: Select one IWT coefficient from the random sequence as IC.
Step 8: Extract last 3 bits of selected IWT coefficient IC and add it into binary stream B.Step 9: If all secret data is retrieved, go to Step 10
Else go to Step 7.
Step 10: Divide binary stream into 7 bits and use 8 bits only for the character whose ASCII valueis greater than 127.
Step 11: Convert all 7-bit or 8-bit blocks into ASCII values and find their respective characters.Step 12: Write all characters into text file secret.txt.
Step 13: Display secret text file - secret.txt.

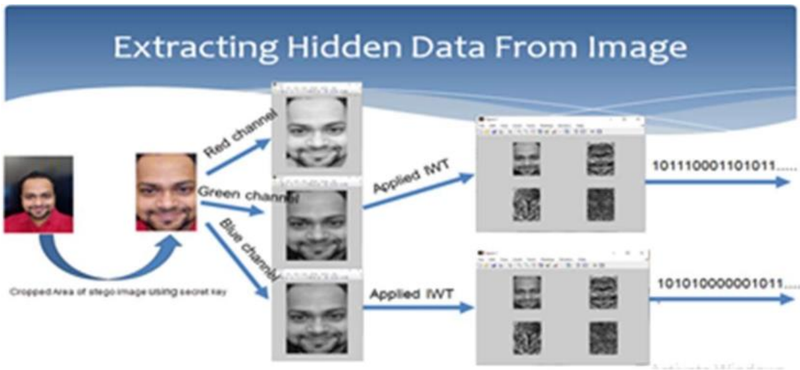

Figure 7 – Process of extracting data from Stego image

Figure 7 shows the extraction process. While extracting data from the image, skin tone area is cropped from stego image with the help of secrete key. The blue, green and red channel of cropped area is separated. The IWT frequency transformation is applied only on blue and green channels of the cropped area. Lastly, the 3 least significant bits of HH, HL sub-band of blue channel and HH sub-band of green channel is retrieved to generate a message stream.

4. Result Analysis

Figure 8 - Step by step output of the proposed method

Figure 8 shows the output of skin tone detector, cropped area, stego image, and generated secret key. At the receiver side this key is used to extract secret data.

Table 2- Difference between Payload capacity of 7-bit and 8-bit representation

Image	7-bit payload capacity (A)	8-bit payload capacity (B)	Difference (A-B)	Raised capacity in %
IMG_1	127203	111303	15900	12.50 %
IMG_2	218021	190768	27253	12.50 %
IMG_3	409942	358,699	51243	12.50 %
IMG_4	740,277	647,742	92535	12.50 %
IMG_5	27,972	24,476	3496	12.50 %
IMG_6	88,498	77,436	11062	12.50 %
IMG_7	61,714	54,000	7714	12.50 %
IMG_8	388,908	340,294	48614	12.50 %
IMG_9	1,919,931	1,679,940	239991	12.50 %
IMG_10	191,738	167,771	23967	12.50 %

Text data is embedded using 7-bit representation to increase payload capacity. Table 2 shows the difference between the payload capacity of 7-bit and 8-bit representation. This table also shows that capacity increased by 12% using 7-bit representation.
Table 3 shows the PSNR and MSE of the proposed method. The proposed method achieves a good PSNR value.
The proposed method provides more security by chosing random sequence to hide data in the image. The randperm() function is used to generate random sequence. Suppose 6 value passed to randperm(6) then it generates random sequence which includes number beween 1 and 6. The number of possible sequences using vlaue 6 is 6! i.e 720. In the proposed method, random sequences are generated using numbers between 1 and the total size of the cropped area. In case of IMG_1 the cropped area is 15,768. So the number of possible sequences genenarated using randperm() function is 15,768!. So, it is challenging for attackers to find the correct sequence of data hiding from the number of possible sequences.

Table 3- PSNR and MSE of Proposed method

Image	Size of cover image in	Size of secret image in	PSNR	MSE

	bytes	**Bytes**		
IMG_1	180,842	26,888	68.1972	0.0098483
IMG_2	615,000	26,888	68.1972	0.0098483
IMG_3	934,880	26,888	66.6208	0.014158
IMG_4	1,942,528	26,888	70.3034	0.0060638
IMG_5	913,725	26,888	62.0997	0.040097

The figure 9 shows the GUI (Graphical User Interface) of the proposed method.

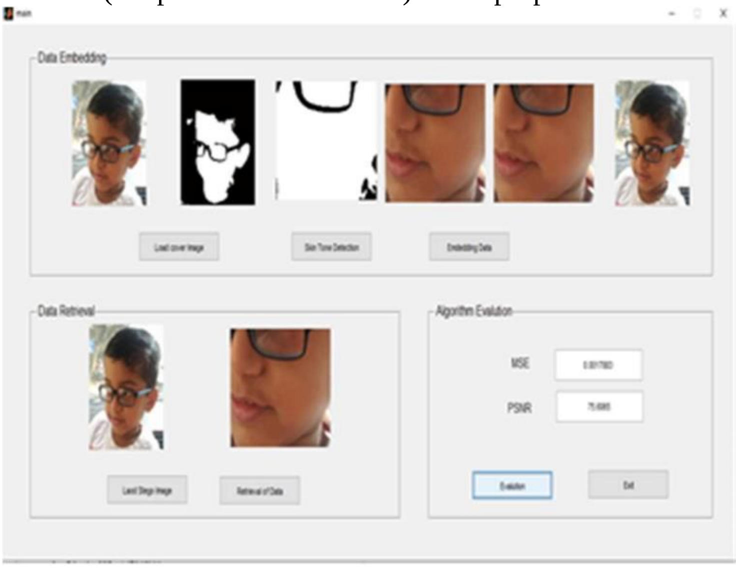

Figure 9 - GUI Interface of the proposed method

Table 4 shows the difference between our proposed method and Anjali A. Shejul, Umesh L. Kulkarni's method. Our proposed method used the IWT frequency transformation and Anjali A. Shejul, Umesh L. Kulkarni's method used DWT frequency transformation. In both method data is embedded into skin tone region. Our proposed method is better than Anjali A. Shejul, Umesh L. Kulkarni's method in case of capacity, security and also produces less distortion. Our proposed method uses blue and green channel so capacity is more. Using random selection process, the security is increased. Using 2k correction, the distortion is decreased. "A Secure Skin Tone based Steganography Using Wavelet Transform" (Anjali A. Shejul, Umesh L. Kulkarni 2011) method used only blue channel with one high- frequency sub band so it has less embedding capacity than our proposed method. Also, it has usedsequential selection so security is less.

Anjali A. Shejul, Umesh L. Kulkarni proposed a method which used discrete wavelet transformation technique. In this methodfirst skin tone is detected using HVS color space; DWT is applied only on blue channel of skin tone area. Lastly, data is embedded into HH sub band of blue channel. This method also compares the result of cropping and without cropping method.

Table 4 - Comparison of the proposed method with Anjali A. Shejul, Umesh L. Kulkarni's method

Factor	**Our Proposed Method**	**Anjali A. Shejul and Umesh L. Kulkarni's Method**
Frequency transformation	Integer wavelet Transformation (IWT)	Discrete wavelet Transformation(DWT)
ROI	Skin Tone Area (Cropping)	Skin Tone Area (cropping and without cropping)

Sub bands used in embedding	Blue HH and HL and Green HH sub band	Blue HH sub band only
Distortion	Less (using 2^k correction)	More
Capacity	More (Using 3 LSB, 7- bit representation)	Less
Security	More (Using RandomGenerator)	Less

According to the method proposed by Anjali A. Shejul, Umesh L. Kulkarni, the cover size of 356 x 356 and secret image of size 32 x 32 is used for the experiment. The average PSNR in case A (without cropping) is 56.42 and the average PSNR in case B (with cropping) is 49.35. The cover images and secret images of the same sizes compare the above method with our proposed method. Table 5 shows the capacity, PSNR and MSE values calculated using our proposed method. Table 5 shows that the capacity and PSNR of our proposed method is better than the method proposed by Anjali A. Shejul, Umesh L. Kulkarni.

Table 5 - PSNR and MSR of the proposed method with cover image size 356 x 356

Image (356 x 356)	**Capacity of cover image in bytes**	**MSE**	**PSNR**	**Size of Logo**
Image 1	47034	0.04588	61.5146	32 x 32
Image 2	34056	0.046064	61.4972	32 x 32
Image 3	110208	0.051585	61.0056	32 x 32
Image 4	61065	0.043221	61.7738	32 x 32

5. CONCLUSION

The proposed method increases security and embedding capacity. While embedding data pixels are selected randomly. So, it becomes difficult for the attacker to retrieve data. Also, only skin tone region is used to embed data so no one can extract data without proper cropped region coordinates. Most commonly used letters can be represented using 7-bit. Hence, this representation is used for such letters to increase embedding capacity. 8-bit representation is used only for those letters which cannot be represented using 7-bits. Thus, the proposed method can work with all letters. The 2k correction decreases the difference between the original and stego images. Thus, the proposed method achieves good PSNR.

Acknowledgement

Authors are very thankful to Shivaji University, Kolhapur, India for providing the necessary support for this research.

Conflict of Interest: Authors declared they have no conflict of Interest.

6. REFERENCES

1. Cheddad, A., Condell, K., Curran and Kevitt M.: Biometric inspired digital image Steganography, Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg.of Computer-Based Systems (ECBS'08), Belfast, 2008, pp. 159-168 (2008)

2. Behbahani, Y., Ghayour, P., and Farzaneh, A.: Eigenvalue Steganography based on eigen characteristics of quantized DCT matrices , ICIMU: Proceedings of the 5th International Conference on Information Technology & Multimedia at UNITEN (ICIMU 2011) Malaysia (2011)

3. Majunatha, H., Reddy Raja, K.: High capacity and security steganography using discrete wavelet transform', International Journal of Computer Science and Security, pp. 462-472 (2009)

4. Johnson, N., Jajodia, S.: Exploring steganography: Seeing the unseen. Computer', 31(2), pp.26-34 (1998)

5. K, A., Vas, S.: Randomized Steganography in Skin Tone Images, International Journal of Computer

Science, Engineering and Information Technology, 8(2/3), pp.01-08 (2018)
6. Kharade, G., Kamat, K., Kharade, S.: Online Library Package to Boost the Functionality and Usability of the Existing Libraries. International Journal on Future Revolution in Computer Science & Communication Engineering, 5(8), 5–7 (2019)
7. Kharade, G., Kharade, K., Katkar, S.: Cyber Security-A Method of Generic Authentication of Data with Ip Security. International Journal of Information Systems, 9(2), 63–65 (2019)
8. Kharade, S., Kharade, K., Kamat, R., Kumbhar, S.: Setting Barrier to Removable Drive through Password Protection for Data Security. Our Heritage, 68(27), 19–23 (2020)
9. Khodaei, M., Faez, K.: New adaptive steganographic method using least- significant-bit substitution and pixel-value differencing, IET Image Processing, 6(6), pp.677-686 (2012).
10. Marvel, L., Boncelet, C., Retter, C.: Spread spectrum image steganography',IEEE Trans. Image Process. 8 1075–1083 (1999)
11. Manisha, K., Manjusha, B.: Skintone Detection Based Steganography Using wavelet transformation, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (I²IT), Pune, 978-1-5090-2080-5/16 (2016)
12. Masoud N. , Ronak K., Mehdi H.: An introduction to steganography methods. World Applied Programming, Vol (1), No (3), 191-195 (2011)
13. Muhammad, K., Ahmad, J., Rehman, N., Jan, Z., Sajjad, M.: CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method', Multimedia Tools and Applications, 76(6), pp.8597-8626 (2016)
14. Patil, B. , Kharade, K., Kamat, R.: Investigation on Data Security Threats & Solutions. International Journal of Innovative Science and Research Technology, 5(1), 79–83 (2020)
15. Po-Yueh C., Hung-Ju L.: A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 4, 3: 275-290 (2006).
16. Prabakaran, G., Bhavani R., Sankaran, S.: Dual Wavelet Transform in Color Image steganography method, International Conference on Electronics and CommunicationSystem (ICECS - 2014).
17. Pratap M.: Modern Steganographic technique: A survey. International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229- 3345, Vol. 3 No. 9 Sep 2012.
18. Raftari, N., Moghadam, A.: Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm. Sixth Asia Modelling Symposium, 978-0-7695-4730-5 (2012)
19. Rima, G., Lakshmi, V.: Integer Wavelet Transform and Arnold Transform based image steganography with cryptanalysis. Proceedings of the Fourth International Conference on Communication and Electronics Systems (ICCES 2019) IEEE Conference Record # 45898; IEEE Xplore ISBN: 978-1-7281-1261-9 (2019)
20. Shejul, A., Kulkarni, U.: A Secure Skin Tone based Steganography Using Wavelet Transform, International Journal of Computer Theory and Engineering, pp.16-22 (2011)
21. Subhedar, M., Mankar, V.: Current status and key issues in image steganography: A survey, Computer Science Review, 13-14, pp.95-113 (2014)
22. Swapnali, R., Zagade, S., Bhosale A.: Skin Tone Based Secret Data Hiding in Imagesby using DWT Technique's. International Journal of Electronics Communication and Computer Engineering, Volume 5, Issue (4) July, Technovision-2014, ISSN 2249–071X (2014)
23. Yu, J., Yoon, E., Shin, S., Yoo, K.: A New Image Steganography Based on 2k Correction and Edge-Detection. Fifth International Conference on Information Technology: New Generations (itng 2008).