BioGecko

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

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

SonaliPowar*
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
Avastvolumeofinformationistransferredovertheinternetinthedigitalera,posingasecurityandauthenticityc hallenge.Togetoverthesecurityproblem,undetectabledataconcealingis used. Steganography conceals the existence of sensitive information. This paper describes an approach that is secure and has good datahiding capacity. The approach hides text information in the cover image's skin to nearea.Theskintonedetectoralgorithmdetectstheskintonearea,whichis subsequently cropped before the secret information is hidden. To boost payload, 7-bits areemployed to represent text data. The skin tone area of the cover image is transferred into thefrequency domain using integer wavelet transformation (IWT). The embedding method utilizesthe blue channel's HH, HL, and HH sub-bands and even the green channel's HH sub-bands. TheIWT coefficient is chosen using a randomgenerator, which promotes security, and the 2Kcorrection is applied toreduce distortion. ThePNSRresults obtained with this method areacceptable.

Keywords:imagesteganography,IWT,2kcorrection,randompixelselection,skintonesteganography

1. INTRODUCTION

The technique of hiding data into another carrier medium is called as steganogrphy.Goodsteganographyprovidesa largecapacitywithlessimperceptibility.InancientGreekusedwaxtableshide themessage "Thepersonwouldscrapethewaxoffatablet,writeasecretmessageontheunderlyingwoodandagain 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 messageon it. After the hair regrows, a massager is sent to the location where the head is shaved to revealthe secret message. People used invisible ink for writing secret messages during the initial period of the World War II. They also used invisibleforwritingsecretmessagesbetweenlinesoftheinnocentletter.Secretdata was also hidden in the document itself. A clear message was written in the document, butconfidential data was present. By extracting specific position letters, data would be retrieved. To conceal data in digitalsteganography,manycarriermediumssuchastext,image,audio,andvideoareused. The use of an image as a carrier medium is termed as imagesteganography.Manytechnologies such as spatial domain, frequency domain, spread spectrum, masking filtering, distortion, etc., are used to embed datainimages(Patiletal.,2020).
Figure1showsthedifferenttechniquesusedtohidedatintheimage.Thespatialdomainprovidesgood capacity but it is a less secure method. The most popular spatial domain method is LSB.In this method, theleastsignificantbitofpixels are used for embedding the data.Wecanenhancecapacitybyincreasingthenumberofmessagebitsperpixel,butvisualdistortionalsoincre

ases.Inthecaseofthefrequencydomain, different transformations like DCT, DWT, DFT, IWT etc. are used for transforming the coverimagefromthespatialdomaintothefrequencydomain(Kharadeetal.,2019).

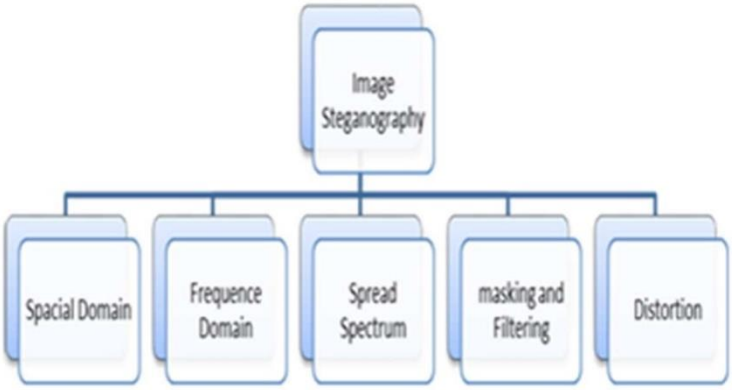

Figure1:ImagesteganographyTechniques

Thefrequency-domaintechniquehaslessembeddingcapabilitybutismorerobustthanthespatialdomain approach. Data is hidden in a specific region rather than the entire image to increasesecurity.Thissortofsteganographyisknownasregion-basedorobject-basedsteganography.Skintone steganography is region-based steganography in which data is only embedded in the skin tonearea.

The spread spectrum image steganography concept is "spreading bandwidth of narrow signalacross a wide band of frequencies" (Subhedar, M. and Mankar, V., 2014). Marvel et al has invented the spread spectrumimage steganography. It is difficult to detect a narrow band signalafter being spread across a wide frequency band. The resulting signal is embedded into the coverimagetoobtainthestegoimage.Becausethepowerofthecoverimageissignificantlygreaterthan thepoweroftheembeddedsignal,theSNR(signaltonoiseratio)islow.WhentheSNRis low,itindicates that the perceptibility is low. A good synchronization of the pseudo-random noisegenerators at both the transmitter and the receiver is required. Otherwise, the desired results willnot 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 andcompressionalso.

The masking and filtering technique is similar to watermarking. It creates marks in the coverimage. In this technique, it is hidden into more significant areas instead of hiding data in noiselevel. This technique does not change image visual properties so that image change should not benoticed with the naked eye (MasoudNosrati, et al.2011). The advantage of this method is, morerobust against compression than LSB method as data is hidden invisible parts of an image. Thedisadvantage is this technique is mainly applied only on gray scale or 24-bit images (PratapChandraMandal,2012).

Thedistortiontechniqueisun-blindimagesteganography.Itmeanstoextractsecretmessageswerequire cover image and stego image. The decoding function checks the difference between thecover and stego image to extract secret messages. "Encoder adds a sequence of change to coverimage. So, information is described as being stored by signal distortion" (H.S. Majunatha Reddyand 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 techniqueisthatwehavetosendacoverimageandstegoimage.

(Po-YuehChenandHung-Ju Lin2006)ProposedamethodinwhichDWTtransformationisusedand low-frequency sub-band LL is kept untouched to maintain image quality. Data is embeddedin two modes fixed (fixed bits per pixel) or variable. While embedding, a key matrix is generatedwhich is also embedded in the image. Data cannot be extracted without the key matrix. ThismethodgivesgoodPSNRvaluesfor highercapacity.

(Shejul and Kulkarni, 2011) use skin tone region to hide data. HVS colour space is used to detectskintonearea. The cover image is transferred into the frequency domain by using DWT.Theskinpixel'sDWT coefficient contains secret data hidden in one of the high-frequency sub-

bands of the DWTcoefficient. Their study looked at both cropping and non-cropping methods and concluded thatcropping provides more security while non-cropping preserves histogram. This method producesimageswithexcellentquality(Shejul,A.andKulkarni,U.2011).

(Behbahani, Ghayour and Farzaneh, 2011) Proposed a method in which an 8X8 DCT quantizedblock is divided into 2X2 sub-blocks. Each submatrix has an eigenvalue and eigenvector. Bychanging these attributes, secret data is embedded in DCT coefficient of image. This methodprovidesresistanceagainstsubtractivepixeladjacencymatrix(SPAM)butitprovideslowpayloadcapacity(KhodaeiandFaez,2012)proposedamethodbasedonLSBsubstitutionandPVD. This technique partitions the cover image into 1x3non-overlapping blocks. Using the optimal bitsubstitution method, K-bits are stored into the central pixel called the base pixel. The differencebetween the new value of base pixel and the value of other two pixels is used to calculate thenumberofbitsthatcanbe storedintotheothertwopixels(Khodaei,M.andFaez,K.2012).

(Prabakaran G. et al. 2014) uses IWT as well as DWT transformation so-called as dual wavelettransformation.Thistechniqueprovideshighcapacityandsecurityandalsoincreasesperformance.

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 goodimagequality(PrabakaranGetal.2014).

(M. Kude and M. Borse 2016) uses HVS color space to find skin tone area. The secret image ishiddeninbluepanelofskintonearea.Beforehiding,thecoverimageisconvertedintoafrequencydomain using Haar-DWT. Only LL sub-band of the secret image is used for the embeddingprocess. This method works with any type of image format. This method gives better PNSR andMSEvalues(ManishaKudeetal.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 whichchannel contains data using a single channel that serves as an indicator. As a result, payloadcapacityisreducedbecauseonlyonechannelisusedtoembeddata(Muhammadetal.,2016).

(KandVasP,2018)detectsskinareausingYCbCrcolourspace.Insteadofhidingdatasequentially,thepixelsarerandomlyselectedusingapseudo-randomgenerator.Thedataishiddenin LSB bit of randomly selected pixel. This method provides good PNSR value i.e. good imagequality. Also, the MSE value calculated using this method is less. So this method is more robust(K,A.andVasP,S.2018).

2. RELATEDWORK

2.1 SKINTONEDETECTION

Instead of hiding data in the whole image, the skin tone area of the image is used to hide data. Ifdata 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 pixelswhoserange ofCris140to165,therange ofCbis140to195,andtherangeofhueis0.01to0.1aretreatedasskinpixelsandnon-skinpixelsotherwise.

FollowingequationsareusedtofindcbandcrvaluesofRGBimage

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)

InaboveequationIisRGBimage.I(:,:,1)representsRedpanel,I(:,:,2)representsGreenpanelandI(:,:,3)representsBluepanel.

FollowingMATLABfunctionisusedtoconvertRGBimageintoHVSimg_hvs=rgb2hsv(img_org);

CROPPING

Skin tone area is cropped before applying IWT. Cropping provides more security (Swapnali R etal.) as without a secret key no one can extract secret data (Shejul et al.. 2011). The area whichcontainsalargeamountofskinpixelsiscropped.

2.2 INTEGERWAVELETTRANSFORMATION

IWT is a lossless transformation technique. In this technique, the original image is reconstructedagain without distortion when reverse transformation is applied. This cannot be achieved usingDWTorDCT.InDCT,theimageisdividedinto8X8pixelblocksandtheDCTisappliedoneach8X8 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 coefficientprovideshighimperceptibilityandincreasesrobustness"(Raftari,N.,2012).WhenIWTisappliedonan imagefoursub-bandsarecreatedLL,LH,HL,HHrespectively(RimaVGetal.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). Thisproducesthefollowingfourparts:

a) LL(HorizontallyandVerticallyLowPass),
b) LH(HorizontallyLowPassandVerticallyHighPass)
c) HL(HorizontallyHighPassandVerticallyLowPass)
d) HH(HorizontallyandVerticallyHighPass).

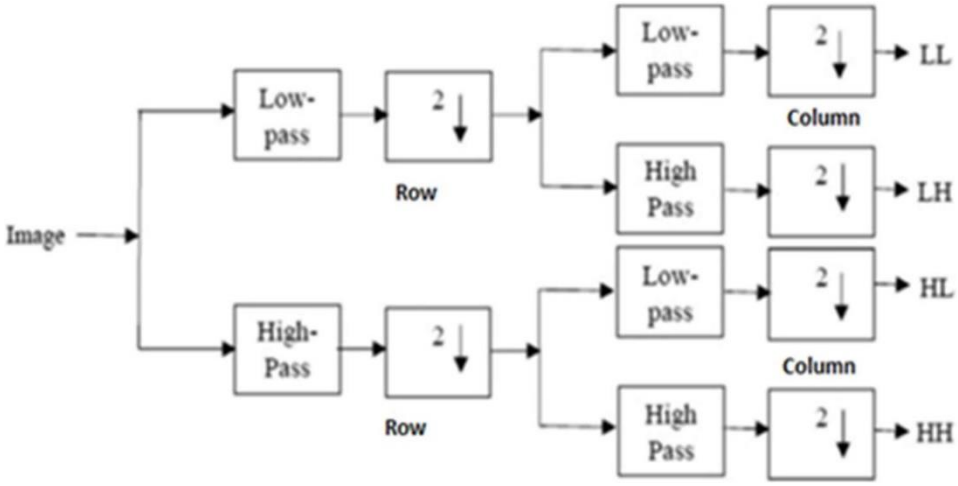

Figure 2 - Filtering used in wavelet transformation

Intheproposedmethod,skintoneareaisusedtohidesecretdata.Theredchannelcontributesmore in skin tone area so it is not used embedding process. So, IWT is applied only on blue andgreenchannels.

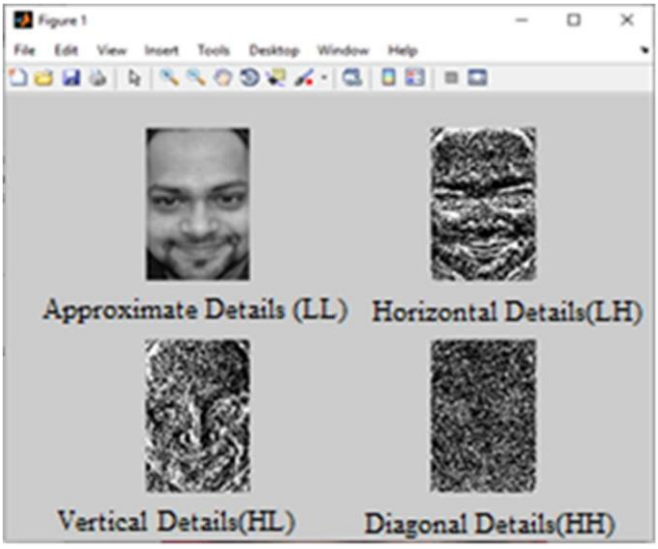

Figure 3 – LL, LH, HL, HH Sub-bands of blue channel

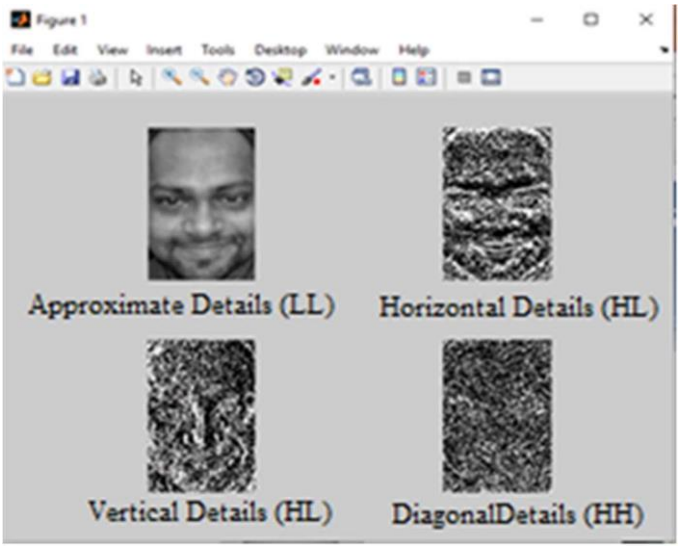

Figure 4 – LL, LH, HL, HH Sub-bands of green channel

Figure 3 and figure 4 shows the LL, LH, HL and HH Sub-bands of blue and green channel. LLsub-band is an approximate sub-band that carries more information about the image. So, changesmadeinLLsub-bandcausemoredistortioninoriginalimage.TheproposedmethodusesHH,HLofblueandHHsub-bandofgreenchanneltocarrysecretinformation.

2.3 SECRETTEXTPROCESSING

The proposed method hides text into the cover image. Table 1 shows the characters whose asciivalueisinbetween1and127.ThemostcommonlyusedcharactershaveASCIIvaluesbetween1and127.So,only7-bitsaresufficienttorepresenttheseletters.Thismethoduses7-bitrepresentation for characters whose ASCII value is less than 127. The 8-bits are only used forcharacterswhoseASCIIvalueisinbetween128and255.So,thismethodworksforallcharacterswhose ASCII value is between 1 and 255. This concept increases embedding capacity to someextent.Table1showscharacterswhoseASCIIvalueisbetween1and127with8-bitrepresentation.Inthiscase,theleftmostbitis'0'.So,thereisnoneedtoembeditintothecoverimage(Kharadee tal.,2019).

Table1.CharacterASCII(1to127)valuetable.

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

2.4 The2kCorrection

Intheproposedmethod3leastsignificantbits(LSB)areusedtohidedata.In2Kcorrection,k means the numberof bits usedindata hidingprocess. "2k correction provides bette
imperceptibility" (Yu, J., Yoon, et al. 2008). After hiding data in 3 least significant bits of IWTcoefficient, 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 hidedata.SoPossiblerangeoferroris

-(2k -1) <=error <=(2k -1)

i.e.-7to+7asthevalueofkis3.

If the difference is greater than 2k-1 then 2k correction is applied to reduce error. In the

proposedmethod,iftheerrorisgreaterthan4(ask=3so23-1=4)then8(ask=3so23=8)issubtractedfromthenewIWTcoefficientvalue.Ifanerrorisnegative,add8intothenewIWTcoefficient.

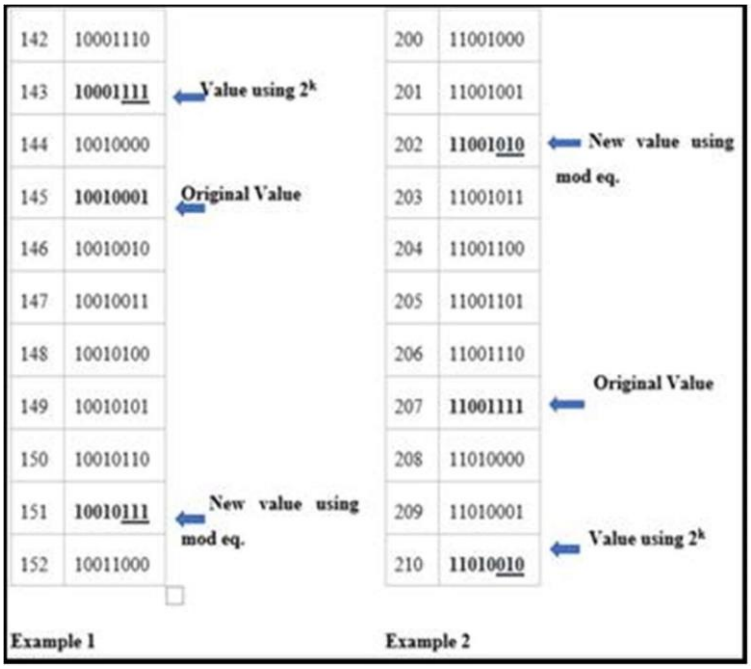

Figure 5: working of 2k correction method

Figure 5 shows the working of 2k correction method. In first example, the original value of IWTcoefficientis10010001(145indecimal)andafterhidingsecretdata111itbecomes10010111(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,thedifferenceispositiveso8issubtractedfromnewcoefficientandtheresultantvalueis1001111(143 in decimal). After appling 2k correction the difference becomes 2(145-143). The originalvalue is 11001111(i.e. 207) in the second example. After hiding data 010, the resultant value is11001010 (202). In the case of the second example, the difference is -5 (202-207) so to reducethis,the8valueisaddedintothenewcoefficienttogetanupdatedcoefficientvalue.Theupdatedcoefficientvalueis11010010(i.e.210)andthenew differencebecomes3only(210-207).

3. PROPOSED METHOD

This method uses IWT (Integer Wavelet Transformation) to transfer an image from the spatialdomaintothefrequencydomain.Beforeembeddingdata,someoperationsareappliedonthecoverimage like preprocessing, skin tone detection, cropping and transformation. At the end, randompixelsequenceisgeneratedtoembeddata.

3.1 EMBEDDINGPROCESS

The skin tone area of the cover image is detected, cropped, and preprocessed to avoid overflowandunderflowproblems.IWTisappliedonblueandgreenchannelsofthecroppedarea.TheHHandHLsub-bandsofthebluechannelandonlyHHsub-bandofthegreenchannelisusedtoembedsecret information. IWT coefficients are randomly selected, 3 secret bits are embedded into 3rightmostbitsoftheselectedIWTcoefficient,and2kcorrectionisappliedtoreducethedifference(Kharadeet al.,2020).

AlgorithmtoEmbeddata intheskintoneareaofthecoverimage:

Input:Coverimage,secrettextmessageOutput:Stegoimage,Secretkey

Step1:SelectcoverimageCandthesecretdatafile.

Step2:DetectskintoneincoverimageCusingaskintonedetectionalgorithm.

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 getIWTcoefficients.UseHH,HLsub-bandcoefficientsofbluechannelandHHsub-bandcoefficientsofthegreenchannel.
Step5:Createabinarystreamofsecretdatausing7-bitrepresentationforcharacterswhoseASCIIvalue is less than 128 and 8-bit representation for characters whose ASCII value is greater than127.
Step6:Ifthelengthofsecrettext>payloadofthe coverimage,then goto13Elsegoto7
Step 7: Sequentially select three bits 'x' from the secret binary stream and randomly select IWTcoefficient'IC'.
Step 8: Hide selected bits 'x' into selected 'IC' using equation IC' = IC – IC mod 2k + x. Apply 2kcorrectiontoreducedistortion.
Step9:IfsecretdataisoverthengotoStep10Elsegotostep7
Step 10: Apply inverse IWT on blue and green channel and combine Red, updated Green andupdatedbluechanneltogetupdatedcroppedRGBimage.
Step11:Mergeupdated croppedareawith coverimageCtoget finalstego image.
Step 12: Generate secret key using position of cropped rectangle in cover image and length ofmessage.
Step13:Stop.

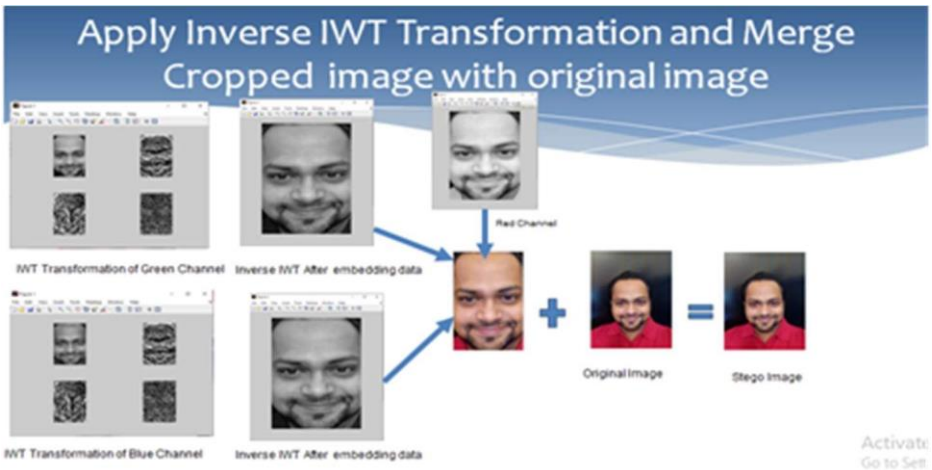

Figure 6 – Process of Embedding data in skin tone area of cover image:

Figure6showstheprocessofhidingdataintoskinareausingproposedmethod.ThedataishiddenintoHLandHHsubbandofbluechannelandHHsubbandofgreenchannel.Aftercompletionofdata hiding process, inverse IWT is applied on blue and green channels. The updated blue andgreenchanneliscombinedwiththeredchanneltogetacroppedRGBimagecontainingconfidentialdata.Lastlycroppedimageismergedwiththeoriginalimagetogetstegoimage.

3.2 EXTRACTIONPROCESS

A secret key is required to extract secret data from stego image. The length of secret data iscalculatedusingsecretkeyandskintoneareaisalsocroppedusingsecretkey.ThenIWTisappliedonblueandgreenchannelsofthecroppedarea.Finally,thebitstreamiscreatedbyextractinglast3bitsoftherandomlyselectedIWTcoefficient.Afterextractingallsecretbits,dividethebitstreaminto 7 bits for characters having ASCII value less than 128 and divide into 8 bits whose ASCIIvalue is greater than equal to 128. Convert all 7 bits and 8 bits blocks into ASCII value and thenfindtheirrespectivecharacter.Finally,writeallthecharactersinthefilesecret.txtanddisplayfilesecret.txt.

AlgorithmtoextractdatafromStegoimageInput:Stegoimage,secretkey
Output:secrettextmessageStep1:Selectstegoimage.
Step2:Usingsecretkey,croptherectangleareafromstegoimage.Also,calculatethelengthofsecrettext.

Step3:Extractblueandgreenchannelsfromthecroppedareaandapply IWTonittogetIWTcoefficients.
Step4:UseIWTcoefficientsofHH,HLsub-bandsofbluechannelandHHsub-bandofgreenchannel.
Step5:Generatesamerandomsequenceof IWTcoefficientlikesenderusingrng()andrandperm()MATLABf unction.
Step6:SetbinarystreamB="orblank.
Step7:Selectone IWTcoefficientfromtherandomsequenceas IC.
Step8:Extract last3bitsofselectedIWTcoefficient IC andaddit intobinarystreamB.Step9:Ifallsecretdataisretrieved,gotoStep10
ElsegotoStep7.
Step10:Dividebinarystreaminto7bitsanduse8bitsonlyforthecharacterwhoseASCIIvalueisgreaterthan12 7.
Step11:Convertall7-bitor8-
bitblocksintoASCIIvaluesandfindtheirrespectivecharacters.Step12:Writeallcharactersintotextfilesecret. txt.
Step13:Displaysecrettextfile-secret.txt.

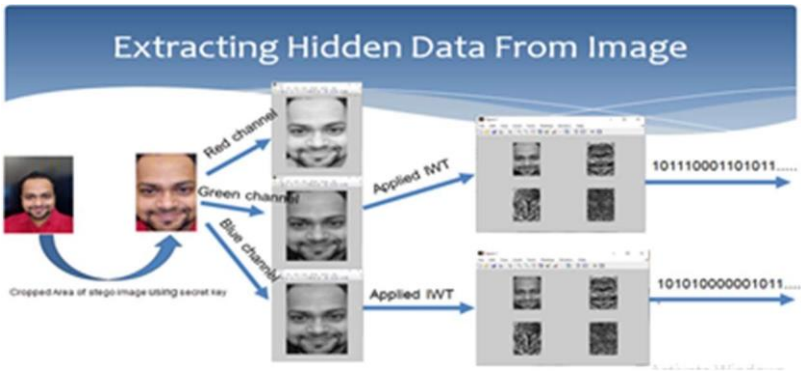

Figure 7 – Process of extracting data from Stego image

Figure 7 shows the extraction process. While extracting data from the image, skin tone area iscroppedfromstegoimagewiththehelpofsecretekey.Theblue,greenandredchannelofcroppedarea is separated. The IWT frequency transformation is applied only on blue and green channelsof the cropped area. Lastly, the 3 least significant bits of HH, HL sub-band of blue channel andHHsub-bandofgreenchannelisretrievedtogenerateamessagestream.

4. ResultAnalysis

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

secretkey.Atthereceiversidethiskeyisusedtoextractsecretdata.

Table2-DifferencebetweenPayloadcapacityof7-bitand8-bitrepresentation

Image	**7-bitpayloadcapacity (A)**	**8-bitpayloadcapacity (B)**	**Difference(A-B)**	**Raisedcapacity 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 thedifference between the payload capacity of 7-bit and 8-bit representation. This table also showsthatcapacityincreasedby12%using7-bitrepresentation.
Table3showsthePSNRandMSEoftheproposedmethod.TheproposedmethodachievesagoodPSNRvalue.
The proposed method provides more security by chosing random sequence to hide data in theimage. The randperm() function is used to generate random sequence. Suppose 6 value passed torandperm(6) then it generates random sequence which includes number beween 1 and 6. Thenumber of possible sequences using vlaue 6 is 6! i.e 720. In the proposed method, randomsequences are generated using numbers between 1 and the total size of the cropped area. In caseof IMG_1 the cropped area is 15,768. So the number of possible sequences genenarated usingrandperm() function is 15,768!. So, it is challenging for attackers to find the correct sequence ofdatahidingfromthenumberofpossiblesequences.

Table 3- PSNR and MSE of Proposed method

Image	**Sizeofcoverimagein bytes**	**Sizeof secretimagein Bytes**	**PSNR**	**MSE**
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

Thefigure9showsthe GUI(GraphicalUserInterface)oftheproposedmethod.

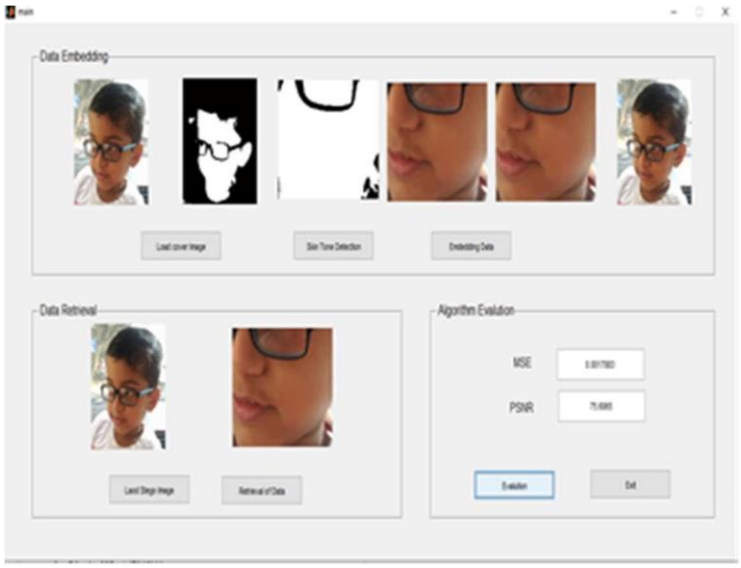

Figure9-GUIInterface oftheproposedmethod

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'smethodusedDWTfrequencytransformation.Inbothmethoddataisembedded 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 proposedmethod uses blue and green channel so capacity is more. Using random selection process, thesecurityisincreased.Using2kcorrection,thedistortionisdecreased."ASecure SkinTonebasedSteganographyUsingWaveletTransform"(Anjali A. Shejul, Umesh L. Kulkarni 2011)methodusedonlybluechannelwithonehigh-frequencysubbandsoithaslessembeddingcapacitythanourproposedmethod.Also,ithasusedsequentialselectionsosecurityisless.
AnjaliA.Shejul,UmeshL.Kulkarniproposed amethodwhich used discrete wavelet transformation technique. In this methodfirst skin tone is detected using HVS color space; DWT is applied only on blue channel of skintonearea.Lastly,dataisembeddedintoHHsubbandofbluechannel.Thismethodalsocomparestheresultofcroppingandwithoutcroppingmethod.

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

Factor	**OurProposedMethod**	**AnjaliA.ShejulandUmeshL.Kulkarni'sMethod**
Frequencytransformation	IntegerwaveletTransformation(IWT)	DiscretewaveletTransformation(DWT)
ROI	SkinToneArea(Cropping)	SkinToneArea(croppingandwithoutcropping)
Subbandsusedinembedding	BlueHHandHLandGreenHHsubband	BlueHHsubbandonly
Distortion	Less (using2^k correction)	More
Capacity	More (Using 3 LSB, 7-bitrepresentation)	Less
Security	More(UsingRandomGenerator)	Less

According to the method proposed by Anjali A. Shejul,Umesh L. Kulkarni, thecoversizeof356x356andsecretimageofsize32x32isusedfortheexperiment.The average PSNR in case

A (without cropping) is 56.42 and the averagePSNR in case B (with cropping) is 49.35. The cover images and secret images of the same sizescompare the above method with our proposed method. Table 5 shows the capacity, PSNR andMSE values calculated using our proposed method. Table 5 shows that the capacity and PSNR ofour 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 (356x356)	**Capacityofcover imagein bytes**	**MSE**	**PSNR**	**SizeofLogo**
Image1	47034	0.04588	61.5146	32x32
Image2	34056	0.046064	61.4972	32x32
Image3	110208	0.051585	61.0056	32x32
Image4	61065	0.043221	61.7738	32x32

5. CONCLUSION

The proposed method increases security and embedding capacity. While embedding data pixelsare selected randomly. So, it becomes difficult for the attacker to retrieve data. Also, only skintone region is used to embed data so no one can extract data without proper cropped regioncoordinates.Mostcommonlyusedletterscanberepresentedusing7-bit.Hence,thisrepresentationis used for such letters to increase embedding capacity. 8-bit representation is used only for thoseletters which cannot be represented using 7-bits. Thus, the proposed method can work with allletters. The 2k correction decreases the difference between the original and stego images. Thus,theproposedmethodachievesgoodPSNR.

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 digitalimageSteganography,Proceedingsofthe15thAnnualIEEEInternationalConferenceandWorkshops ontheEngg.ofComputer-BasedSystems(ECBS'08),Belfast,2008,pp.159-168(2008)
2. Behbahani,Y.,Ghayour,P.,andFarzaneh,A.:EigenvalueSteganographybasedoneigen characteristics of quantized DCT matrices , ICIMU: Proceedings of the 5th InternationalConference onInformationTechnology&Multimedia atUNITEN(ICIMU2011)Malaysia(2011)
3. Majunatha, H., Reddy Raja, K.: High capacity and security steganographyusing discrete wavelet transform', International Journal of Computer Science and Security, pp.462-472(2009)
4. Johnson,N.,Jajodia,S.:Exploringsteganography:Seeingtheunseen.Computer',31(2),pp.26-34(1998)
5. K,A.,Vas,S.:RandomizedSteganographyinSkinToneImages,InternationalJournalofComputerScience ,EngineeringandInformationTechnology,8(2/3),pp.01-08(2018)
6. Kharade, G., Kamat, K., Kharade, S.: Online Library Package to BoosttheFunctionalityandUsabilityoftheExistingLibraries.InternationalJournalonFutureRevolutioninC omputerScience&CommunicationEngineering,5(8),5–7(2019)
7. Kharade, G., Kharade, K., Katkar, S.: Cyber Security-A Method ofGeneric 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 BarriertoRemovableDrivethroughPasswordProtectionforDataSecurity.OurHeritage,68(27),19–23 (2020)
9. Khodaei, M., Faez, K.:New adaptive steganographic method using least-significant-bitsubstitutionandpixel-valuedifferencing,IETImageProcessing,6(6),pp.677-686 (2012).
10. Marvel, L., Boncelet, C., Retter, C.:Spread spectrum image steganography',IEEETrans.ImageProcess.81075–1083 (1999)

11. Manisha, K., Manjusha, B.: Skintone Detection Based Steganography Usingwavelettransformation,InternationalConferenceonAutomaticControlandDynamic 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 steganographymethods.WorldAppliedProgramming,Vol(1),No(3),191-195 (2011)
13. Muhammad, K., Ahmad, J., Rehman, N., Jan, Z., Sajjad, M.: CISSKA-LSB:colorimagesteganographyusingstegokey-directedadaptiveLSBsubstitutionmethod',MultimediaToolsandApplications,76(6),pp.8597-8626 (2016)
14. Patil,B.,Kharade,K.,Kamat,R.:InvestigationonDataSecurityThreats&Solutions. InternationalJournalofInnovativeScience andResearchTechnology,5(1),79–83 (2020)
15. Po-YuehC.,Hung-JuL.:ADWTBasedApproachforImageSteganography,InternationalJournalofAppliedScienceandEngineering4,3:275-290 (2006).
16. Prabakaran, G., Bhavani R., Sankaran, S.: Dual Wavelet Transform in ColorImagesteganographymethod,InternationalConferenceonElectronicsandCommunicationSystem(ICECS-2014).
17. PratapM.: ModernSteganographictechnique:Asurvey.International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345,Vol.3No.9Sep2012.
18. Raftari, N., Moghadam, A.: Digital Image Steganography Based on IntegerWaveletTransformand AssignmentAlgorithm.SixthAsiaModellingSymposium,978-0-7695-4730-5 (2012)
19. Rima,G.,Lakshmi,V.:IntegerWaveletTransformandArnoldTransformbasedimage steganography with cryptanalysis. Proceedings of the Fourth International Conference onCommunicationandElectronicsSystems(ICCES2019)IEEEConferenceRecord#45898; IEEEXploreISBN:978-1-7281-1261-9 (2019)
20. Shejul, A., Kulkarni, U.: A Secure Skin Tone based Steganography UsingWaveletTransform, InternationalJournalofComputerTheoryandEngineering,pp.16-22 (2011)
21. Subhedar,M., Mankar,V.: Currentstatusandkeyissuesinimagesteganography:Asurvey,ComputerScienceReview,13-14,pp.95-113 (2014)
22. Swapnali, R., Zagade,S., BhosaleA.:SkinToneBasedSecretDataHidinginImagesby using DWT Technique's. International Journal of Electronics Communication and ComputerEngineering,Volume5,Issue(4)July,Technovision-2014,ISSN2249–071X (2014)
23. Yu,J.,Yoon,E.,Shin,S., Yoo,K.: ANewImageSteganographyBasedon2kCorrectionandEdge-Detection.FifthInternationalConferenceonInformationTechnology:NewGenerations(itng2008).