American Journal of Engineering Research (AJER)

e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-3, Issue-8, pp-101-112
www.ajer.org

Research Paper Open Access

DWT-AES BASED INFORMATION SECURITY SYSTEM FOR UNMANNED VEHICLES

Renjith V Ravi[1] Dr.R. Mahalakshmi[2],
[1](Ph.D Research Scholar, Karpagam University, Coimbatore, India)
renjith_v_ravi@yahoo.co.in
[1](Professor and HOD, Dept. of EEE, Sree Krishna College of Technology, Coimbatore, India)

ABSTRACT: *Security of data is crucial in present day telecommunication framework, AES algorithm is one of the prominent methods for information Encipherment. For secure image communication needed for unmanned robotics, Discrete Wavelet Transform (DWT) is embraced for image decomposition, quantization and determination of appropriate sub bands is needed to precede encryption and to decrease execution time. In this paper, a modified algorithm for secure image encoding is proposed, demonstrated and is examined for its execution. Different images are considered as experiments for encoding, with parallel operation of AES algorithm the aggregate time in encoding the image is decreased to 2 seconds (evaluated focused around programming reference model). PSNR for different images acquired exhibit the exhibitions of the proposed model for image encoding. Image size of 1024x1024 is considered for encryption and unscrambling. The results got exhibit the exhibitions of AES algorithm.*

KEY WORDS : *DWT, AES cryptography, software model of AES, image encryption*

I. INTRODUCTION

One among the most mainstream momentum research territory in civil and defense is unmanned robotics. Adjustments of self-sufficient vehicles are developing particularly in provisions, for example, producing, perilous materials taking care of, observation, remote sensing, and protection part and country security. The fundamental errand in any such requisition is the view of the surroundings through one or more sensors overwhelmingly by utilizing image sensors. Unmanned robotics is eagerly being produced for both non military person and military utilization to perform dull, grimy, and unsafe exercises. These unmanned vehicles (UVs) are remote-worked and the vehicles are controlled by a human administrator through a communications join. Control movements are dictated by the administrator based upon either coordinate visual perception or remote review through a Polaroid. Since computerized feature or images taken from UVs transmission framework generally incorporates a packing module that intends to decrease the transmitted bit rate. Throughout transmission over an open communication join encryption of compacted information is extremely critical and consequently the cryptography strategies must be precisely outlined. In this work, encryption of the image is completed utilizing specific key while getting the first image the same key is utilized. Information exchange through open system is constantly unsecured, in this way security is one of the significant difficulties that need to be tended to guarantee the dependable information exchange. The security issue in this manner turns into an imperative issue in today's wired or remote Internet provisions. A standout amongst the most helpful systems to secure information is utilizing a cryptographic framework, as the outline of figure algorithms is focused around a propelled numerical hypothesis. It generally blends distinctive sorts of cryptosystems in a safe convention to give a safe channel to information transmission. As a rule, asymmetric-key crypto frameworks, and RSA stands for Rivest, Shamir and Adleman who first freely depicted it in 1978. Symmetric-key crypto frameworks, for example, Data Encryption Standard (DES) or Advanced Encryption Standard (AES), are utilized to encrypt mass data in the transmission stage. Because of restricted figuring assets in compact requisitions, the framework normally off-burdens the security methodology to devoted unique hardware. As of late, there have been numerous chips away at outlining savvy encryption hardware utilized as a part of versatile provisions [1]–[10].

A few works [1]–[5] concentrate on territory diminishment of AES, while others [6]–[10] propose to lessen hardware cost for both ECC and RSA crypto frameworks. Image processing is discovering essentialness in different provisions as after most recent 10 years. Interactive media requisitions are ruled by image processing. It is obligatory to secure or ensure sight and sound substance from unapproved access. Securing the image or video content in a sight and sound data is of essential imperativeness as image passes on more data than whatever available wellspring of data. Images are huge in size and oblige expansive capacity unit, consequently encryption of image substance is additionally drawn out [14]. Conventional encryption algorithm set aside a few minutes expending for huge size of image data, henceforth encryption algorithms ought to be altered for bigger image sizes and need to be quicker. [13,14,15] reports that symmetric key algorithm have computational time short of what asymmetric key algorithms. Symmetric key algorithms, for example, AES, DES have been effectively utilized for encryption of data, hardware algorithms for AES have made them quick and consequently expend less time, however for images with extensive data size AES is still prolonged. Image processing is discovering vitality in different provisions as following the time when most recent 10 years. Multimedia requisitions are commanded by image processing. It is required to secure or ensure multimedia content from unapproved access. Ensuring the image or video content in a multimedia data is of essential significance as image passes on more data than any viable wellspring of data. Images are expansive in size and oblige huge storage unit, consequently encryption of image substance is likewise time intensive [12]. Conventional encryption algorithm set aside a few minutes devouring for extensive size of image data, consequently encryption algorithms ought to be modified for bigger image sizes and need to be speedier. [11, 12, 13] reports that symmetric key algorithm have computational time short of what asymmetric key algorithms. Symmetric key algorithms, for example, AES, DES have been effectively utilized for encryption of data, hardware algorithms for AES have made them quick and consequently spend extremely less time, however for images with huge data size AES is still lengthy. In [14, 15, 16] fast symmetric architectures for hardware execution of AES algorithm is accounted for. These algorithms have not been approved for image encoding. A focal attention for any cryptographic framework is its vulnerability to conceivable strike against the encryption algorithm, for example, measurable ambush, differential assault, and different animal assaults. Lapses in channel likewise degenerate the encrypted data and thus there is a requirement for suitable strategy that could be utilized to distinguish and right the mistakes. In this paper, we investigate the exhibitions of AES algorithm for different inputs, keys and commotion in channel. Execution investigation completed aides in distinguishing a suitable mistake redressing algorithm for AES.

II. RELATED WORK

Secured image encoding is one of the novel methodologies that have been embraced in UVs for data transmission to the base station. The input image caught by the UVs is transformed utilizing Discrete Wavelet Transform (DWT) to get different sub bands, the sub bands are quantized and the quantized sub bands are encrypted. The encoding strategy, for example, Huffman encodes the encrypted data and compresses the data caught, and is transmitted to the base station. Figure 1 shows the block diagram of secured image coding [17]. DWT has been generally utilized as a part of numerous diverse fields of audio and video signal processing. DWT is constantly progressively utilized as compelling answers for the issue of image compression. Quantizer is the procedure of approximating the continuous set of values in the image data with a finite set of values. The outline of the quantizer has a critical effect on the measure of compression got and loss caused in a compression plan. AES is a block cipher with variable key length (128-bit, 192-bit, and 256-bit separately) and block size of 128-bit. AES require low memory to make it extremely appropriate for confined space situations, in which it additionally shows great execution. Huffman coding is a manifestation of encoding that makes the most productive set of prefix codes for a given content. The standard is to utilize a lower number of bits to encode the data that happens all the more as often as possible. The controller is a module required for improving provisions security prerequisites based on a variable framework assets.

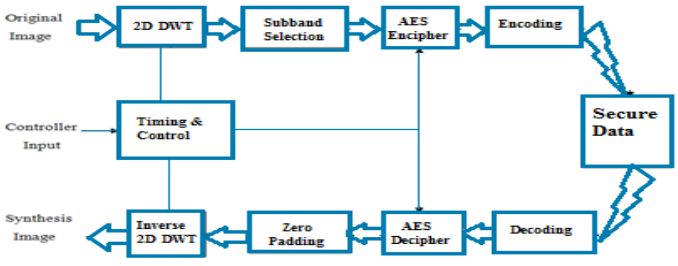


Figure 1 Secure Image Codec[17]

Clients can characterize their security necessities for a specific security benefit by indicating a security range. G. Liu, T. Ikenaga, S. Goto and T. Baba in their paper have proposed another video security scheme , which incorporates two encryption methods. The conspicuous feature of this system is a shuffling of AC occasions produced after DCT transformation and quantization stages [18]. DCT presents blocking ancient rarities and thus, DWT is received. M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki [19], in their paper, they dissected the Advanced Encryption Standard (AES), and they include a key stream generator (A5/1, W7) to AES to guarantee enhancing the encryption execution; mostly for images portrayed by diminished entropy. Equipment implementation of DWT with encryption forces significant difficulties and have been examined in [20][21][22],[23]. In this paper we investigate the execution of secure image coding utilizing software reference model.

A. Two Dimensional Discrete Wavelet Transform for Image Compression

The two dimensional DWT is turning into one of the standard apparatuses for image fusion in image and signal processing field. The DWT methodology is done by progressive low pass and high pass filtering of the digital image or images. This methodology is known as the Mallat algorithm or Mallat-tree decomposition. Figure 2 shows an implementation structure of the 2-D DWT-IDWT. The primary level of transformation is performed along the rows and the second level of transformation happens along the column. The four sub band segments (LL, LH, HL and HH) catch the low frequency parts (DC part), high frequency segments (edges along vertical, horizontal and diagonal axis). On the reverse process, the original image is reconstructed based on inverse transformation methodology utilizing IDWT.

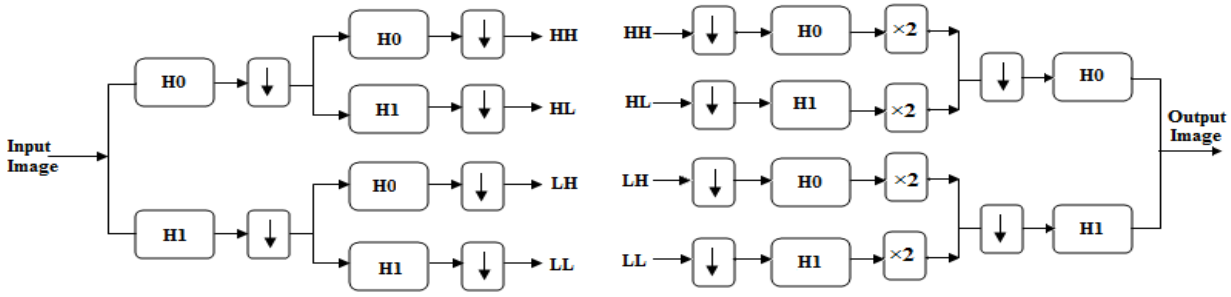


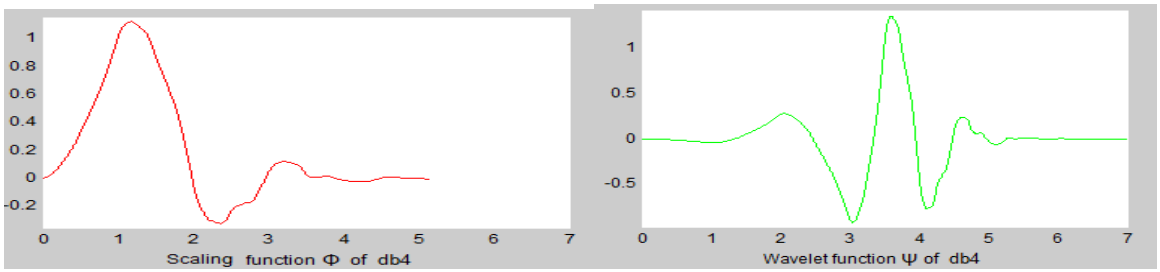
Figure 2 Analysis and synthesis filter bank structure of DWT

For perfect reconstruction, the coefficients for the high pass and low pass filters needed to satisfy the following two properties shown in Eq. 1 and Eq. 2 respectively .

$$\frac{1}{2}\left[H_0\left(z^{1/2}\right)X\left(z^{1/2}\right)+H_0\left(-z^{1/2}\right)X\left(-z^{1/2}\right)\right] \quad \text{....Eq. (1)}$$

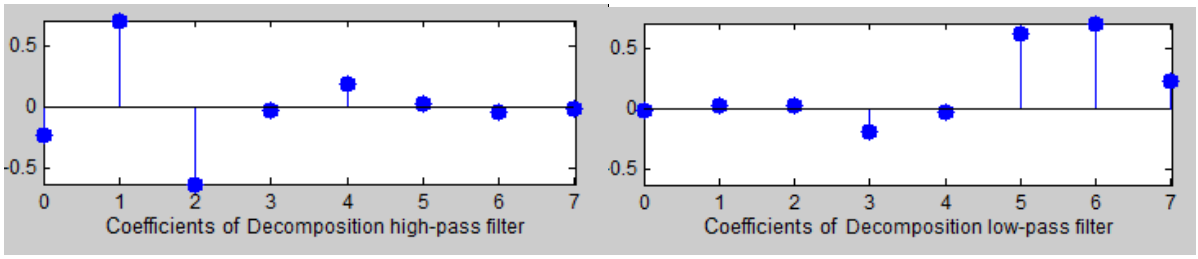
$$\frac{1}{2}\left[H_1\left(z^{1/2}\right)X\left(z^{1/2}\right)+H_1\left(-z^{1/2}\right)X\left(-z^{1/2}\right)\right] \quad \text{....Eq. (2)}$$

The discrete wavelet transform used in this work is Daubche's db4 wavelet. Figure 4(a) and 4(b) shows its scaling and wavelet functions respectively.and Figure 5; (a),(b),(c) and (d) shows the coefficients of its decomposition and reconstruction lowpass and high pass filters respectively.

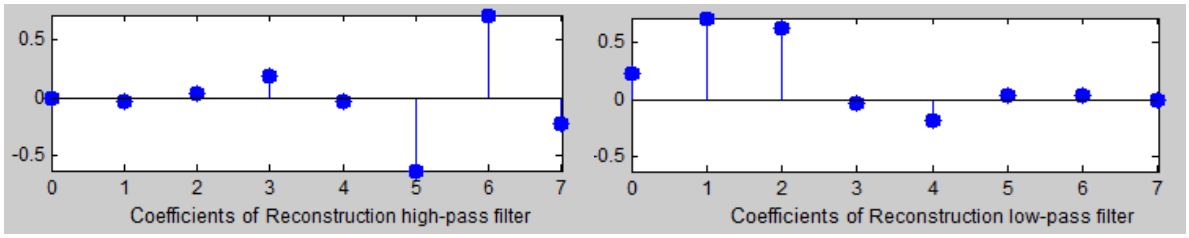


(a) (b)

Figure 4 Scaling and wavelet functions of db4 ; (a) Scaling function of db4 , (b)Wavelet Function of db4



(a) (b)



(c) (d)

Figure 5 Decomposition; (a) high pass filter, (b) Low pass filter; Reconstruction filters; (c) high pass filter, (d) Low pass filter

Figure 3(a) shows the general concept for image decomposition using dwt . In the first level, input image is disintegrated into four sub bands (LL,LH,HL, HH), the LL sub band part is further decayed into four more sub band segment in the second level. figure 4 shows the pyramidal decomposition of input image utilizing DWT.In Figure 4(a) shows the input image, Figure 4(b) shows the aftereffects of first level decomposition, Figure 4(c) shows the second level decomposition stage and Figure 4(d) shows the synthesized image. The information is really display in the LL sub band the other three sub bands give information on edges of a given protest in the original image.

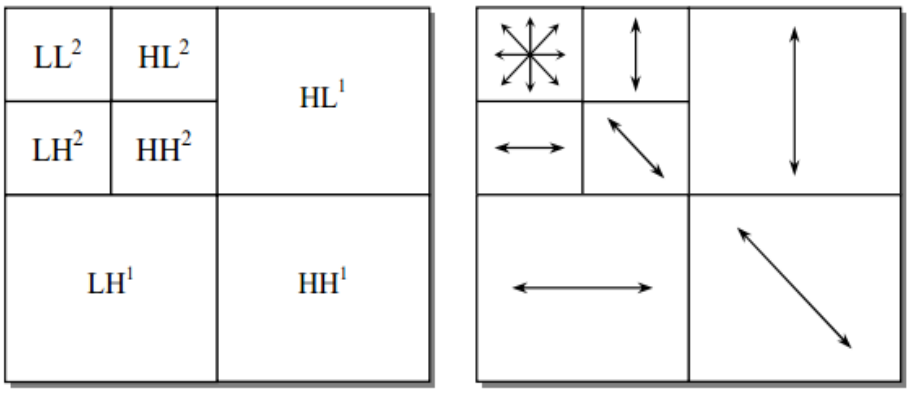
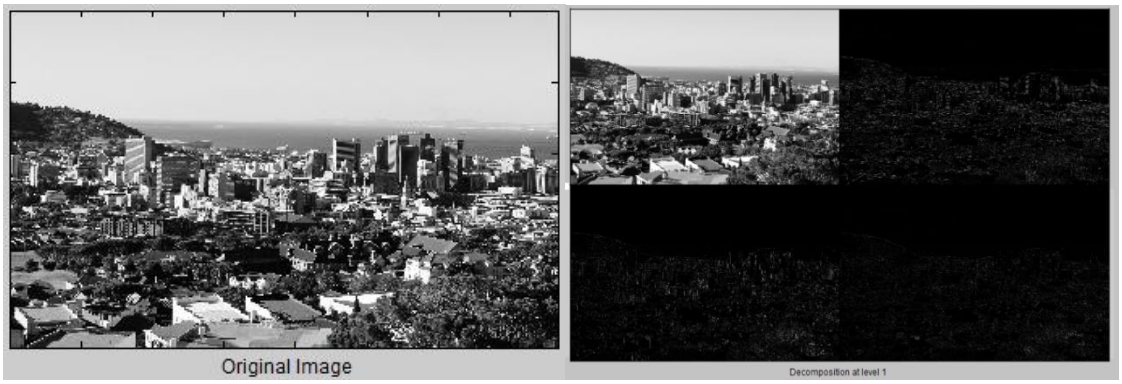


Figure 6 shows the general concept for image decomposition using dwt.

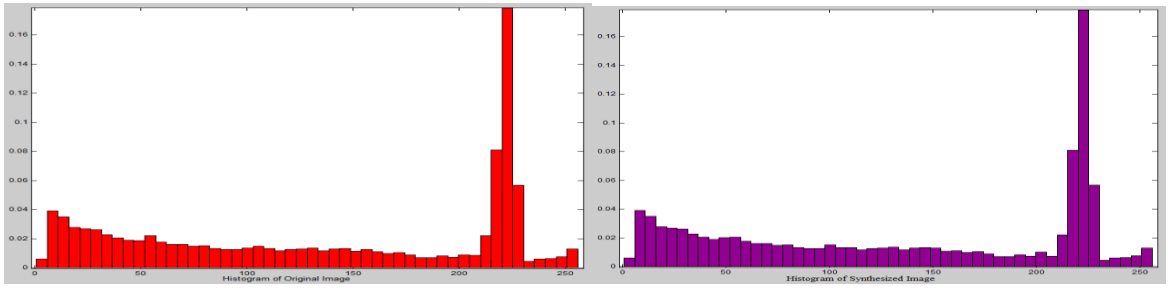


(a) (b)

(c) (d)

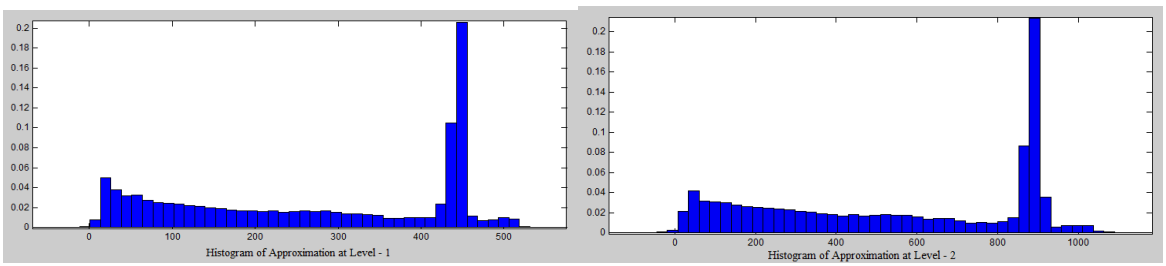
Figure 7 Image decomposition reconstruction of DWT; (a) Original Image (b) 1st level decomposition (c) Second level decomposition (d) synthesized Image

Figure 5 shows the histograms of original and synthesized image. These two histograms are almost same. Figure 6 shows the histograms of approximation components at level 1 and level 2, those are having slight difference. Figure 7, 8, and 9 are the histograms of horizontal, vertical and diagonal components at level 1 and level 2 respectively, these are significantly different from each other.



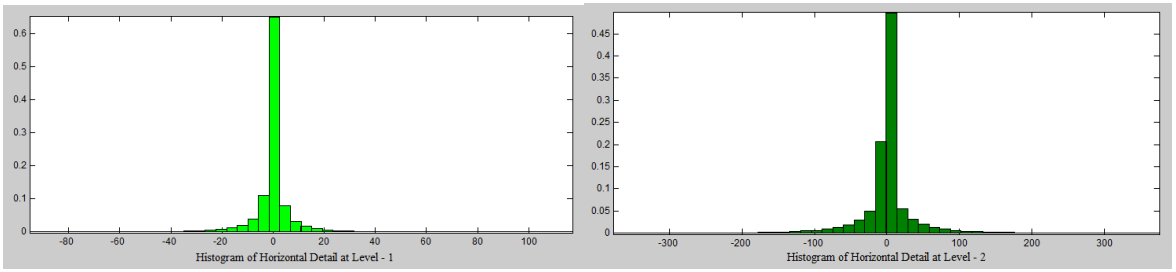
(a) (b)

Figure 8 Histograms of original image and synthesized image; (a) Histogram of original image,(b)Histogram of Synthesized Image



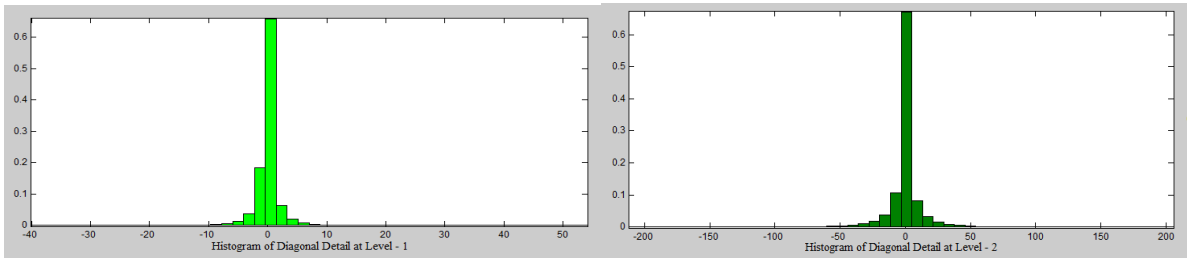
(a) (b)

Figure 9 Histograms of Approximation components; (a) at level 1, (b) at level 2



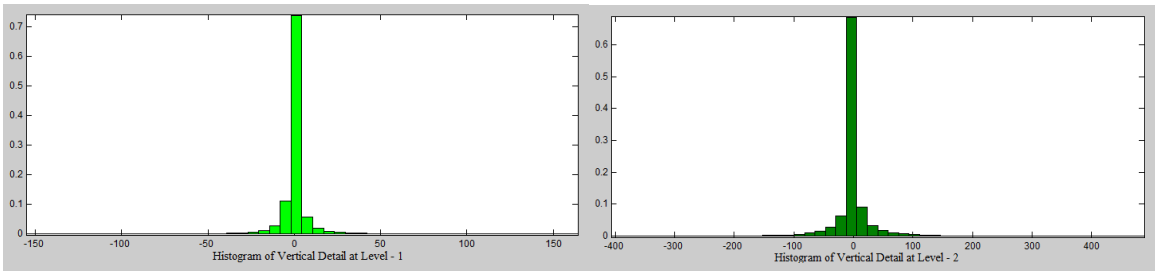
(a) (b)

Figure 10 Histograms of Horizontal components; (a) at level 1, (b) at level 2



(a) (b)

Figure 11 Histograms of Diagonal components; (a) at level 1, (b) at level 2



(a) (b)

Figure 12 Histograms of Vertical components; (a) at level 1, (b) at level 2

Image compression is accomplished by quantizing the higher sub bands that are not exceptionally noteworthy and transmitting the LL sub band without quantization. An input image of size N x N after two level decomposition will offer ascent to 7 sub bands (three more elevated amount sub bands of size N/2 x N/2 at the first level, three N/4 x N/4 at the second level and one low frequency sub band of N/4 x N/4). Image compression is accomplished by picking just the noteworthy sub bands that give information and quantizing all other sub bands.

B. Advanced Encryption Standard

Advanced Encryption Standard (AES) is a symmetric block cipher that methodologies data blocks of 128 bits utilizing the cipher key of length 128, 192, or 256 bits. The AES algorithm [2] composes the data block in a four row and row-significant requested matrix. The first AES encryption/ decryption system is demonstrated in Figure 5. In both encryption and decryption, the AES algorithm utilizes a round function, which comprises of four distinctive byte situated transformations:

[1] Sub Bytes substitutes each one State of the data block with a substitution table (S-box) estimation of that byte.
[2] Shift Rows shifts the each one row of the state cluster by distinctive counterbalances cyclically, and the counterbalance relies on upon row-list.

[3] Mix Columns transforms every section of the matrix by multiplying it with a consistent GF polynomial.
[4] Add Round Key adds a Round Key to the State by a straightforward bit wise XOR operation.

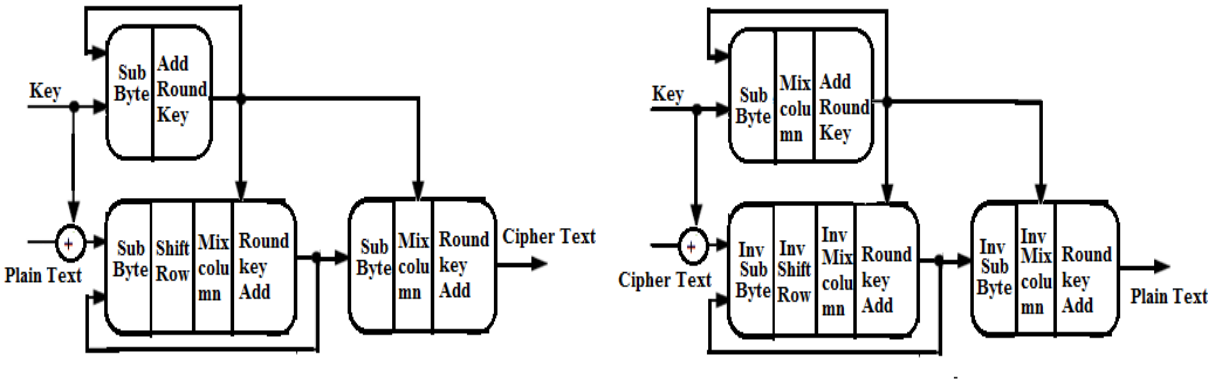


Figure 13 AES Encryption and Decryption

In AES algorithm, every 128-bit data is masterminded as a 4 x 4 state, worked by four primitive transformations. Throughout the encryption/decryption transform, the four primitive transformations are executed iteratively in Nr rounds, where the estimation of Nr will be 10, 12, or 14, contingent upon which key size is chosen. In the encryption technique, the approaching data will first be bit wise XORed with an introductory key, and afterward, four transformations are executed in the accompanying request: Sub-Bytes, Shiftrows, Mix columns, and Add Round key. Recognize that the Mix Columns transformation is not performed in the last round. The execution grouping is turned around in the decryption process, where their converse transformations are Inv Sub bytes, Inv Shift Rows, Inv mix columns, and Add Round key, individually. Since each one round needs a round key, a beginning key is utilized to create all round keys before encryption/decryption. In the AES algorithm, the Sub bytes transformation is a nonlinear byte substitution made out of two operations: 1) 1) Modular inversion over GF(28), modulo an irreducible polynomial p(x) = x8 + x4 + x3 + x + 1 and 2) affine transformation characterized as y= mx +v, where M is a 8 x 8 b matrix, v is a 8-b constant, and x/y indicates 8-b data/yield. In the Mixcolumns transformation, the 128-b data organized as a 4 x 4 state are worked column by column. The four components of every column structure a four-term polynomial that is multiplied by a constant polynomial C(x) = {03} x3 + {01}x2 + {01}x + {02} modulo x4 + 1. The Shift Rows transformation is a basic operation in which each one line of the state is cyclically shifted right by different offsets. The Add Roundkey transformation is a bitwise XOR operation of each one round key and current state.

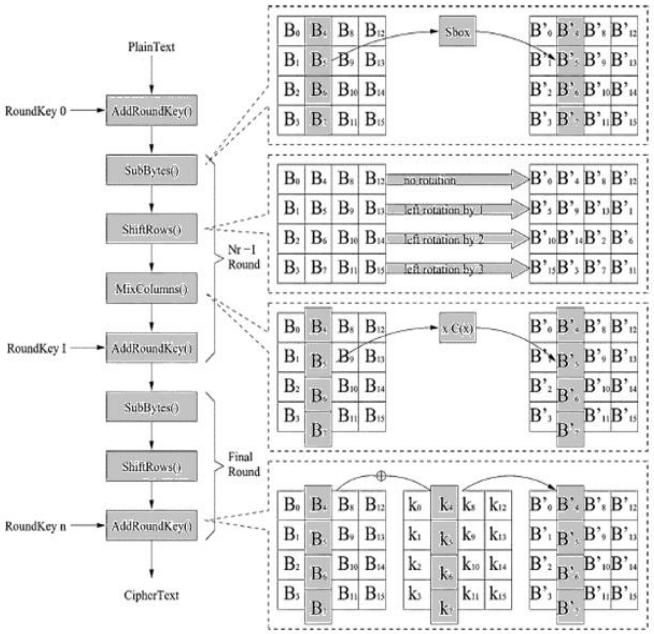


Figure 14 AES algorithm

The creation of s-box functioned in two steps, first finding the multiplicative inverse of the element over Galois Field GF(2^8) modulo and the irreducible polynomial given in Eq. 1

$$x^8 + x^4 + x^3 + x + 1 \text{ ---------- Eq.1}$$

Second, apply affine transformation of the structure y = Mx + C to the inverse , where M = 8 x 8 bit matrix , C = 8-bit constant and x/y = 8-bit input/output. Shift rows implies cyclic shift of each one column to the left by a predefined offset as demonstrated in Figure 14. Mix column works on every column exclusively. Every byte is mapped into another value which is a function of each of the 4 bytes in that column. In Add Round Key, the 128 bits of state are bit wise XORed with 128 bits of the round key. Each one round key generated in the key expansion and scheduling process. 10 rounds of the entire AES process are rehashed for a key length of 128 bit. The round keys are generated by a key expansion process. The expanded key is 176 bytes in length. Software modeling of AES encryption algorithm utilizing Matlab has been completed and different transformations utilized as a part of the algorithm in changing over plain text to cipher text were examined. The software modeling has been completed such that the main program calls the initialization function and the encryption function which thus calls other sub functions to fulfill the undertaking of encryption. Next segment talks about the software model for AES algorithm.

III. PROPOSED METHOD FOR SECURE IMAGE CODING

The real limits saw in image encoding are the aggregate computation time in AES algorithm when connected to image data (16,384 frames). So as to lessen the computation time , input image is transformed to sub bands utilizing DWT and each one sub band is quantized and encoded utilizing AES. The computation time is reduced and likewise is more suitable for real time provisions. The modified block diagram for secure image encoding is demonstrated in Figure 15. In the modified algorithm the input image is decomposed into 7 sub bands of high and low frequency components . The LL2 sub band is encoded utilizing AES algorithm. The other sub bands are LH2, HL2 and HH1 are picked and quantized. Consequently the picked sub bands are scrambled utilizing AES algorithm independently. The aggregate number of bits that are encoded after 2D DWT and quantization are demonstrated in Table 1.

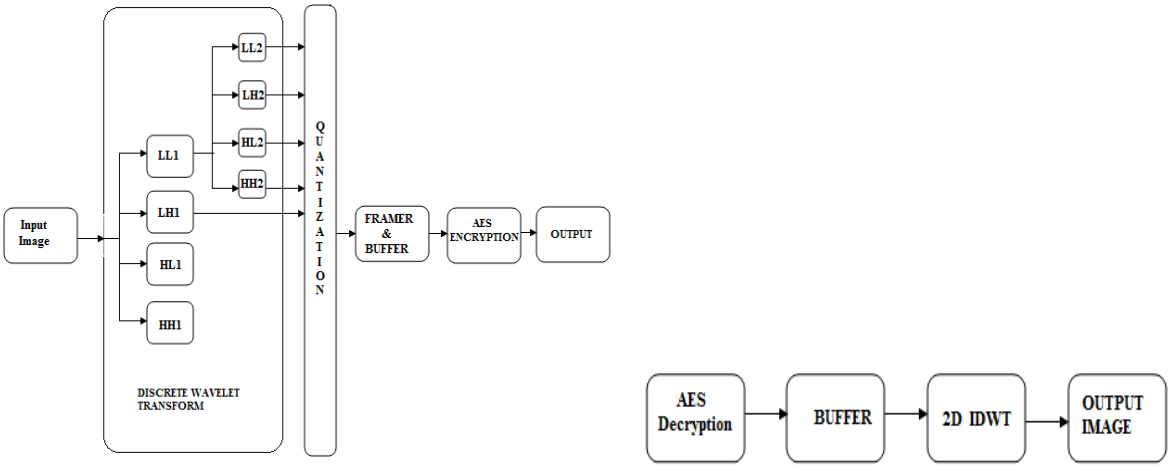


Figure 15 Modified Secure Image Encoding Transmitter and Receiver; (a) Transmitter (b) Receiver

In the modified encoding scheme LH2, HL2 and HH1 are picked as they hold the high frequency components of the input image along the vertical, horizontal and diagonal directions. The vertical component and horizontal component information is caught from the second level decomposed sub band, the diagonal component is caught structure the first level sub band component. Further, the Ll2 component might be decomposed to four more sub bands in the third level and suitable sub band components could be quantized and encoded utilizing AES algorithm freely.

TABLE 1 NUMBER OF BITS AND FRAMES IN PROPOSED METHOD

Input Image Size	Bits per frame	LL2/LH2/HL2 /HH2 size (in No. of bits)	LH1/HL1/HH1 size (in No. of bits)	No. of bits to be encoded using AES after selection
64 x 64	32768 (256)	2034	9126	15228 (119)
128 x 128	131072 (1024)	9126	36864	64242 (502)
256 x 256	524288(4096)	36864	147456	258048 (2016)
512 x 512	2097152(16384)	147456	589824	1032192(8064)

The table 1 shown above presents the number of bits encrypted using AES algorithm for different image sizes. In the image encoding scheme without DWT, the number of frames to be encoded (each of 128 bits), are shown in brackets in column 2. After decomposition using 2d-DWT using two level, the number of frames to be encoded is shown in brackets in column 5. After DWT, the pixels are spoken to using 9 bits. The aggregate number of frames to be encrypted after DWT is diminished by half accordingly the computation time for AES algorithm is lessened to short of what 8 seconds (16 seconds is the time without DWT). As the AES algorithm is encoding the sub bands independently, the aggregate time for encoding is short of what 2 seconds in the altered algorithm.

IV. RESULTS AND DISCUSSION

The modified algorithm proposed is demonstrated utilizing Matlab and is confirmed for its usefulness utilizing different test images. Figure 8 shows the test images considered for encryption and decryption. The info image is decomposed into sub bands and the sub bands are encrypted utilizing AES algorithm, the encrypted information is decrypted and inverse DWT is connected to acquire the first image. Top Signal to Noise Ratio (PSNR) is registered to gauge the exhibitions of the encryption plan.

Figure 16 Test images for secure encoding

The software reference model created in Matlab, performs DWT of each one image and the decomposed sub bands are taken and focused around the information accessible in the sub bands. The picked sub bands are quantized and encrypted. The quantization process in this work contrasts the sub band coefficients and a threshold, the coefficients beneath threshold are made zero, and coefficients over the set threshold are held. In this work, for the LL2 the threshold is situated to +/ -61, for the LH2 and HL2 the threshold is situated to +/ -136, and for the HH1 the threshold is situated to +/ - 212. The thresholds have been recognized focused around trial and error, so that the information in the decomposed image is not lost. After quantization the information is lost in the decomposed image, however the image size is diminished and along these lines reduces postpone in AES processing. Table 2 shows the PSNR consequences of AES with DWT and without DWT. Quantization process presents losses in the image, without quantization the PSNR is very nearly closer to the PSNR acquired without DWT.

TABLE 2 RESULTS OF PROPOSED METHOD

Test Image	**Without DWT**		**With DWT and Without Quantization**		**With DWT and With Quantization**	
	MSE	**PSNR in dB**	**MSE**	**PSNR in dB**	**MSE**	**PSNR in dB**
Dam	2.307	44.50	3.014	43.34	3.557	42.62
Old street	2.711	43.80	3.909	42.21	4.765	41.35
Office	3.007	43.35	4.286	41.81	5.201	40.97
Flower	1.466	46.47	2.173	44.76	2.723	43.78
Houseboat	1.816	45.54	2.489	44.17	2.898	43.51
Coconut trees	2.455	44.23	3.282	42.97	3.855	42.27
Church	1.941	45.25	2.736	43.76	3.358	42.87
Hill	1.582	46.14	2.005	45.11	2.383	44.36
Valley	2.033	45.05	2.774	43.70	3.428	42.78
Fruits	2.980	43.36	4.286	41.81	5.141	41.02
Cityscapes	2.323	44.47	3.343	42.89	3.954	42.16
Townatnight	1.779	45.63	2.530	44.10	2.979	43.39
Street	1.205	47.32	1.783	45.62	2.114	44.88
Sunset	1.439	46.55	1.968	45.19	2.329	44.46
Shore	2.806	43.65	3.742	42.40	4.53	41.57
Keralasunset	1.225	47.25	1.722	45.77	2.124	44.86
Wind	1.055	47.90	1.626	46.02	1.919	45.30

Boy	2.905	43.50	3.954	42.16	4.689	41.42
Braches	1.200	47.34	1.300	46.99	1.507	46.35
Forest	1.928	45.28	2.972	43.40	3.532	42.65
Fox	2.979	43.39	4.54	41.56	5.371	40.83
Rail	2.345	44.43	2.952	43.43	3.508	42.68
Warehouse	1.775	45.64	2.484	44.18	2.885	43.53
Lake	1.047	47.93	1.497	46.38	1.775	45.64
Cat	0.853	48.82	1.286	47.04	1.556	46.21
Staircase	1.127	47.61	1.479	46.43	1.795	45.59
Vegetables	1.808	45.56	2.637	43.92	3.274	42.98
Grapes	0.893	48.62	1.371	46.76	1.679	45.88

PSNR results got without and with quantization are demonstrated in column 3 and 4 respectively and are contrasted and the consequences of image coding with AES encoding in column 2. The greatest deviation as far as PSNR for the picked images is 4 db and 9 db without quantization and with quantization. To enhance the PSNR and lessen computation time, the input image might be decomposed into various progressive sub bands and quantization threshold could be set fittingly to acquire the first image without misfortune. DWT is performed to decrease computation time in AES encoding on the input image straightforwardly. Further, exhibitions of different DWT filters can likewise be evaluated on the reconstruction process. In this work, Db4 wavelets have been utilized for deterioration and reconstruction. From the results got we exhibit that the decision of DWT channel, choice of sub bands, quantization threshold and parallelism of AES calculation assumes an indispensable part in secure image encoding for Unmanned Vehicles.

VI. CONCLUSION

In this work we have developed a secure image coding scheme with multi level of security based on DWT and AES algorithm and utilized the AES algorithm for the encryption of consistent image information and two dimensional DWT for image decomposition. We have developed a software reference model of DWT, with AES algorithm for security and have proposed a fractional encryption procedure based on AES. Exploiting the DWT in our work, one may decide to encrypt LL band with security level goes from low to high. Expanded protection is exchanged off against more encryption time. The percentage of information subjected to encryption while keeping up medium confidentiality is fundamentally diminished as contrasted with full encryption .The encryption of just LL2 sub band information as of now conveys a fulfilling secure result. The proposed procedure might be utilized as a part of telecommunication between an unmanned vehicle and its base station. Test results exhibit that the proposed secure image encoding scheme is quick and is appropriate to give high security provisions.

REFERENCES

[1] A. E. Rohiem, F. M. Ahmed and A. M. Mustafa "FPGA Implementation of Reconfigurable Parameters AES Algorithm", *13th International Conference on Aerospace Sciences and Aviation Technology, ASAT- 13*, May 26 – 28, 2009.

[2] A. Hodjat, I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA". *Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines* (FCCM'04).

[3] A. Mansouri, A. Ahaitouf, and F. Abdi, "*An Efficient VLSI Architecture and FPGA implementation of High-Speed and Low Power 2-D DWT for (9, 7) wavelet Filter*", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[4] A. Satoh and K. Takano, *A scalable dual-field elliptic curve cryptographic Processor*, IEEE Transactions on Computer Science, Vol. 52, No.4, pp.449–460, 2003

[5] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, *"FPGA implementation of AES Encryption and Decryption"*, International Conference on Control , Automation, Communication and Energy Conservation -2009, 4th-6th June 2009.

[6] Bruce Schneir, Applied Cryptography, 2nd Edition, John Wiley and Sons Publishers, 1996

[7] Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, *An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems*, IEEE Transactions on Very Large Scale Integration Systems (VLSI), Vol.18, No.4, pp.553-563, 2010

[8] D. Dia, M. Zeghid, M. Atri, B. Bouallegue, M. Machhout and R. Tourki, *"DWT-AES Processor for a Reconfigurable Secure Image Coding"*, International Journal of Computer Science and Engineering,vol.1,no.2,june 2009.

[9] D.Dia, M.Zeghid, M.Atri, B.Bouallegue, M.Machhout and R.Tourki, *"DWT-AES Processor for a Reconfigurable Secure Image Coding"*, International Journal of Computer Science and Engineering,vol.1,no.2,june 2009.

[10] Deepthi,H.S.,Manure, S.S. ; Prasanna Raj, C. ; Bhusare, S.S. ; Naik, U.L.*," Design and FPGA implementation of improved lifting scheme based DWT for OFDM systems "*3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011),

[11] Dominik Engel Thomas stutz,Andreas Uhl*,"A survey on JPEF2000 encryption"*, Multimedia systems[online] SpringerLink Verlag pp.1 -29, ,2008.

[12] Flayh, N.A. ; Dep. of Comput. Sc., JMI, New Delhi, India ; Parveen, R. ; Ahson, S.I.*," Wavelet based partial image encryption "*, IEEE International Conference on Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT '09.

[13] G.Liu, T.Ikenaga, S.Goto and T.Baba, *"A Selective Video Encryption Scheme for MPEG Compression Standard"*, in IEICE Transactions on Fundamentals of Electronics, communications and Computer Sciences, 89 (2006), pp. 194-202.

[14] Harris D., Krishnamurthy R., Anders M., Mathew S.,, and Hsu S., *An improved unified scalable radix-2 Montgomery multiplier*, Proceedings of 17th IEEE Symposium on Computer Arithmetic, pp. 172–178, 2005

[15] Herstein I. N., *Abstract Algebra*, Macmillan Publishing Company, 1990

[16] K. Gaj, P.Chodowiec, *"Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays"*, CT-RSA 2001, pp.84-99

[17] K. Janvinen, M. Tominisko, J. Skytta, *"A fully pipelined memorlyess 17, 8 Gpbs AES-128 encryptor"*, in International symposium of Field programmable Gate arrays, 2003, pp.207-215.

[18] M. Mclone, J.V. McCanny, *"Rijindael FPGA implementations utilizing look-up tables"*, J.VLSI signal process, syst. 34(3)(2003)261-275.

[19] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, *"A Modified AES Based Algorithm for Image Encryption"*, International Journal of Computer Science and Engineering,1(2007), pp.70-75.

[20] Manure, S.S. ; M. Tech (VLSI Design & Embedded Syst.), KLECEL, Belgaum, India ; Raj, C.P.P. ; Naik, U.L*," DEsign and performance analysis of DWT/FFT based OFDM systems "*,3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011)

[21] Qibin Hou ; Inst. of Autom., Chinese Acad. of Sci., Beijing, China ; Yangsheng Wang*," Security traffic image transmission based on EZW and AES "* , IEEE Intelligent Transportation Systems(Volume:1), 2003. Proceedings. 2003

[22] Ramanaiah, K.V. ; Narayana Eng. Coll., Gudur, India ; Raj, C.P.*," VLSI Architecture for Neural Network Based Image Compression "*,3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010

[23] Safari, A. ; Dept. of Electron., Macquarie Univ., Sydney, NSW, Australia ; Yinan Kong *," Performance comparison of orthogonal and biorthogonal wavelets using technology libraries "*, 13th International Symposium on Communications and Information Technologies (ISCIT), 2013 .

[24] Satoh A., Morioka S., Takano K., and Munetoh S., *Unified hardware architecture for128-bit block ciphers AES and Camellia*, Proceedings of cryptographic Hardware and Embedded Systems, pp. 304–318, 2003

[25] Shiguo Lian*," Quasi-commutative watermarking and encryption for secure media content distribution"*,[online], Multimedia Tools and Applications Volume 43, Number 1 / May, 2009

[26] Shtewi,A.M. *"An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems"* IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, pp 226-232 February 2010

[27] Sugreev Kaur and Rajesh Mehra*,"High Speed and Area Efficient 2D DWT Processor Based Image Compression"*, Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

[28] Tenca A. F. and Koç C. K., *" A scalable architecture for modular multiplication based on Montgomery's algorithm"*, IEEE Transactions on Computer Science, Vol. 52, No. 9, pp. 1215–1221, 2003

[29] Wang J., Zeng X.,, and Chen J.,*"A VLSI implementation of ECC combined with AES "*, Proceedings of International Conference on Solid State and Integrated Circuit Technology, pp. 1899–1904, 2006

[30] William Stallings, Cryptography and Network Security Principles and Practices, 4th edition, Prentice Hall, 2007