High Performance Security System For Image In IoT

K.Suwetha[1], K.Vinothini[2] and R.Shankar[3]
[1]Department of ECE, JEPPIAAR SRR ENG COLLEGE, swethakumar020@gmail.com
[2]Department of ECE, JEPPIAAR SRR ENG COLLEGE,vinovini76@gmail.com
[3]Associate Professor, Department of ECE, JEPPIAAR SRR ENG COLLEGE,

---

Abstract- Image or video exchange has become one of the important requirements in diverse applications in this Internet of Things era. Quad rotor is one of the applications of IoT. In quad rotor, with Secure Digital Camera images can be captured. After capturing the image, it should be shared with the intended users securely. It is assured by image hiding technique in which a secret image is hidden into another image known as cover image. After embedding the secret image, the cover image only will be appeared. For the secured and long distance transmission of captured images, it is proposed to integrate novel hybrid algorithms with SDC, in this paper, The hybrid algorithms used to integrate with SDC are firefly for image hiding, Lagrange Interpolation for image encryption, Set Partitioning In Hierarchical Tree for compression and Orthogonal Frequency Division Multiplexing for transmission. Thus it is attempted to eliminate privacy and security concerns through the proposed integration of hybrid algorithms with SDC.

Keywords - Internet of things (IoT), Secure Digital Camera (SDC), Firefly Algorithm Lagrange Interpolation, Set portioning in tree hierarchical tree algorithm (SPIHT), Orthogonal Frequency Division Multiplexing (OFDM).

1.INTRODUCTION

Quad rotors are commonly used with an onboard camera and one or two operators. The operators control both the flight of the vehicle and the camera operation. In industrial applications this provides a swift, easy and relatively low-cost means for inspection of pipelines, bridges and large structures and navigating areas that are remote and otherwise hard to access. Civil applications include explore and rescue, traffic congestion analysis, fire monitoring, HAZMAT (hazardous material) operations and the inspection of dangerous sites as well as environmental assessments and nature conservation. In law enforcement they are helpful for surveillance, documenting crime scenes and gathering intelligence. By enabling autonomous control with object recognition and video tracking many of these tasks can be self-operated permitting for more vehicles to be employed with considerably fewer operators. For example, during a search and rescue mission, multiple quad rotors could be programmed to search a given area sending an alert to the search team when a possible subject is found. If they are equipped with an infrared thermal imaging camera this would permitting them to search through the night. Similarly, for law enforcement and surveillance a subject could be tracked by multiple quad rotors, all communicating with the base station or each other, forming a subnet of the IoT. The quad rotor(s) continuously process information from external sources such as GPS and the IoT.

SDC is a novel approach in capturing digital images. A fundamental digital camera is only able to capture digital images and maintain a visual record of events. However, it is not possible to track the source, insure the authenticity and progression of custody for the digital images. Even the use of digital watermarking capabilities cannot provide indisputable authentication of the images. Data loss might also occur in a digital camera. From the above discussions, it is evident that the SDC is arguably one of the best proven appliances of capturing multimedia. It attempts to eliminate privacy and security concerns.

As quad rotors will be widely used in places where it would be hard for direct access, the images obtained need to be completely trusted as a faithful reflection of the exact situation. Images obtained using conventional cameras are more vulnerable to tampering. So they cannot be used for targeting in a quad rotor. For example, when a quad rotor is used for critical applications like documenting a crime scene, if the images are tampered by hackers, then the very purpose of documenting will not be achieved. Similarly, when a quad rotor is used for civil applications like traffic congestion analysis, if secure image processing is not performed, then hackers can easily distort it leading to chaos during important hours of the day. In situations such as environmental assessments, the image can be easily modified by anyone using image editing tools widely available. Hence using a SDC for these applications is very important as there is a need to protect these images against intrusion.

.

2.PROPOSED METHODOLOGY

Images captured in SDC has to be securely transmitted for long distance; it is performed by integrating novel hybrid algorithms with SDC. The hybrid algorithms such as firefly for image hiding, Lagrange interpolation for image encryption, SPIHT for image compression and OFDM for long way transmission are used.

The proposed algorithm offers double-layer protection in form of encryption and image hiding, which addresses issues related to security, privacy and digital rights management (DRM).

The novel contributions are:

- Lossless compression is implemented.
- Less memory space is acquired during image hiding.
- High Peak signal to noise ratio (PSNR) is achieved.
- Low Mean Square Error (MSE) is acquired.

- Reduced Noise is attained for hidden image.
- Quality of the image is improved.

Thus, the SDC with hybrid algorithms is arguably one of the best proven ways to facilitate real time rights management, and is considered to be very suitable for real time applications such as IoT.

2.1) IMAGE HIDING USING FIREFLY ALGORITHM

The firefly algorithm (FA) is an iterative algorithm.The proposed system infers a new frequency domain firefly algorithm based on image hiding technique.The key idea of the technique is twofold: multi resolution representation of image and odd-even quantization. Secret image is embedded into cover image by odd-even quantization in order to modifying coefficients. Secret image is to be hidden into cover image using key image.

I) IMAGE HIDING PROCESS

Cover and secret images are divided into 8x8 size non overlapping blocks. In each iteration,firefly module finds the optimum location.Then each firefly's position is updated using below equation.

$$x_i=x_i+\beta_0(,)+\alpha(rand-1/2) \quad (1)$$

The best location is found when the following conditions occur:

- Number of iteration exceeds maximum number of iterations
- No improvement is obtained in the successive iterations
- An acceptable result has been found

The blocks of secret image is embedded in the best pixel of each cover image block. For this purpose the histogram shifting method is used.

The histogram H(x) is generated based on the formula:

$$H(x) = px \quad (2)$$

The maximum intensity pixel or peak point and minimum intensity pixel or zero point are found in the histogram H(x). Peak point of secret image block is embedded into peak point of cover image block.similarly zero point of secret image block is embedded into zero point of cover image block.

Once this process is completed then the Structural Similarity Index Measure (SSIM) for the cover and embedded image is calculated. Then the BER is calculated.

The Structural Similarity Index Measure is used to calculate the embedded image quality which is defined as follows:

$$SSIM(X,Y)=\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu^2_x+\mu^2_y+c1)(\sigma^2_x+\sigma^2_y+c2)} \quad (3)$$

Where x and y are same size window of the cover and embedded image ux and uy are corresponding x and y averages. Sigma x^2 and Sigma y^2 are the variances of x and y and sigma xy is the x and y's covariance. c1 and c2 are constants.

The Bit Error Rate (BER) represents the robustness of the embedded image is defined as:

$$BER = \sum_{k=0}^{n} b \quad b' / N \quad (4)$$

where b and b' are embedded and extracted bits respectively, N is the total number of secret bits embedded and represents the XOR operation. The value of BER will be anywhere between 0 and 1. If BER value closer to 1 then the error value of extracted image is higher. The main objective of this proposed method is to minimize the bit error rate and maximize the SSIM index.

2.2) IMAGE ENCRYPTION USING LAGRANGE INTERPOLATION

This will provide authentication of users, and integrity, reliability and welfare of images which is travelling over internet. Moreover, an image-based data requires more effort during encryption and decryption.

The Lagrange Interpolation algorithm is used for encryption and decryption of an image transform into cipher code using the random keys, which allow users to have privacy and security in channeling of the image based data as well as in storage in the data warehouse This work has been proved to provide high protection to the images from illegal intrusions. It is swift in the process of encryption and decryption algorithm. The decryption process does not induce any loss of image data, and it has ability of dealing with different format of images as well.

The proposed work contents are as follows

- Send the embedded image to the Encryption function,which calls the procedure Keys(XOR key mapping) to generate the randomly prime number between (1– 256) and keeping it in the form of matrix.
- Initially, divide the embedded image into (n * n) of random block, where n is a value resolute by user.
- Encrypt each embedded block with the keys which are stored in matrix form.

2.3) IMAGE COMPRESSION USING SPIHT ALGORITHM

The conventional image coding technology utilizes the redundant data in an image to compress it. But these methods have been replaced by digital wavelet transform. These methods have peak speed, low memory requirements and absolute reversibility. Now in this work we are considering SPIHT algorithm. We are analogizing it with wavelet encoding scheme and examining the final results in terms of bit error rate, PSNR and MSE

The SPIHT algorithm is more efficient implementation than Embedded Zero Wavelet (EZW) algorithm .

This compression conspiracy is based on wavelet coding technique. The image is transformed using a discrete wavelet transform. In the originating, the image is deteriorated into four sub-bands by cascading horizontal and vertical two-channel

critically sampled filter-banks. After implementing wavelet transform to an image, the SPIHT algorithm partitions the decomposed wavelet into significant and insignificant partitions based on the following function:

Here $S_n(T)$ is the significance of a set of coordinates T, and $c_{i,j}$ is the coefficient value at coordinate (i, j).

There are two passes in the algorithm- the sorting pass and the refinement pass. The SPIHT encoding technique utilizes three lists LIP (List of Insignificant Pixels). It contains individual coefficients that have magnitudes smaller than the thresholds.LIS (List of Insignificant Sets) contains set of wavelet coefficients that are described by tree structures and are found to have magnitudes smaller than the threshold. LSP (List of Significant Pixels) . It is a list of pixels found to have magnitudes greater than the threshold (significant). The sorting pass is performed on the above three lists.

In the refinement pass, the nth MSB of the coefficients in the LSP is the final output. The value of n is decremented. These passes will keep on pursuing until either the desired rate is reached or n =0. The latter case will give an almost perfect renovation since all the coefficients have been processed completely. The bit rate can be controlled absolutely in the SPIHT algorithm as the output generated is in single bits and the algorithm can be completed at any time.

2.4) TRANSMISSION USING OFDM

OFDM is a method of encoding digital data on multiple carrier frequencies. A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels. The low symbol rate makes use of a guard interval between symbols affordable, making it possible to eliminate the Inter symbol interference (ISI) and utilize echoes and time-spreading to achieve a diversity gain, i.e. a signal-to-noise ratio improvement. The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions without complex equalization filters.

i) PROCESS IN OFDM

Initially embedded image is not in a suitable form for direct transmission through OFDM system. For transmitting this image which is available in matrix or two dimensional signals, we need to do some pre-processing for transmuting this 2D image into 1D signal.

- Read the image which is available by default in 1024 x 1024 sizes and represented in uint8 format.
- Convert it into double format and reshape the data to change from matrix representation of 1024 x 1024 into vector representation of 1 x 1048576.

Now we successfully transmuted 2D signal to 1D signal. This signal is now partially ready for transmission purpose. In the final step, relying upon the modulation technique used, we need to convert the vector data into suitable form. For example, if we use BPSK modulation, then we need to convert the vector data into binary data (two signaling elements i.e. 0s and 1s). For QPSK modulation, we need to convert the vector data into binary data (four signaling elements i.e. 00, 01, 10 and 11 respectively).

- Convert the vector data into suitable modulation

The source data which is in serial form is transmuted to parallel form by S/P so as to assign the data onto multiple sub-carriers and modulated by any of the M-PSK or M-QAM Technique.

- After modulation, IFFT operation is performed and finally the signal is converted from parallel form to serial form by using P/S for communication purpose.

- Channelize the image in AWGN channel

At the receiver corresponding inverse operations are performed so as to efficiently recover the transmitted image.

3.RESULTS

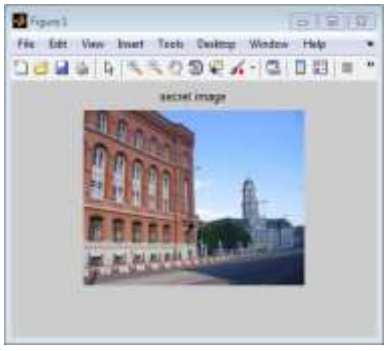

Fig 1.secret image

Fig 2.cover image

Fig 3.Frequency similarity

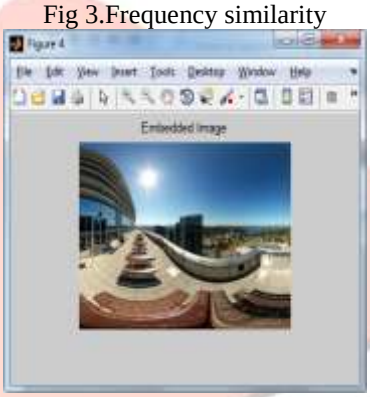

Fig 4.Embedded image

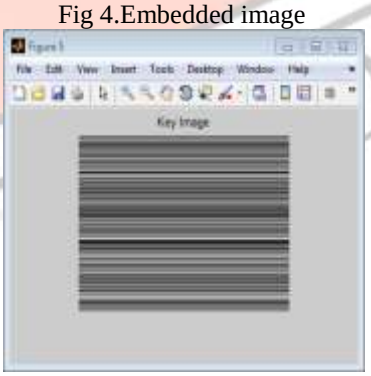

Fig 5.Key image

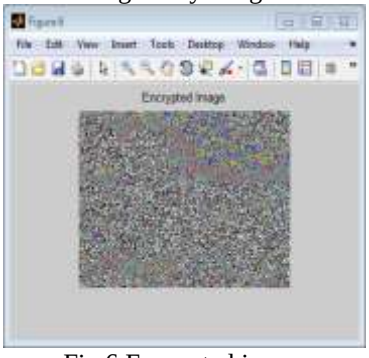

Fig 6.Encrypted image

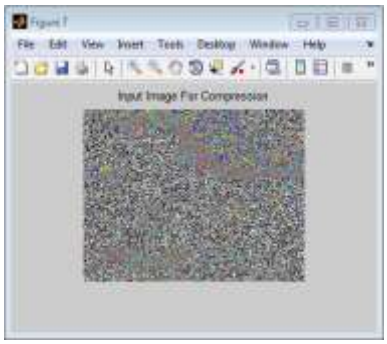

Fig 7.Input Image for Compression

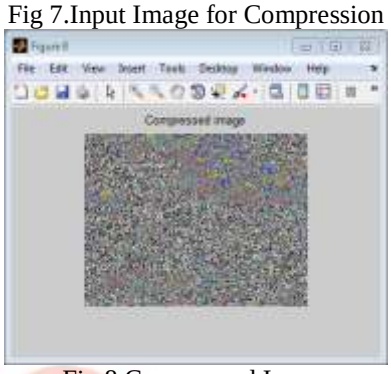

Fig 8.Compressed Image

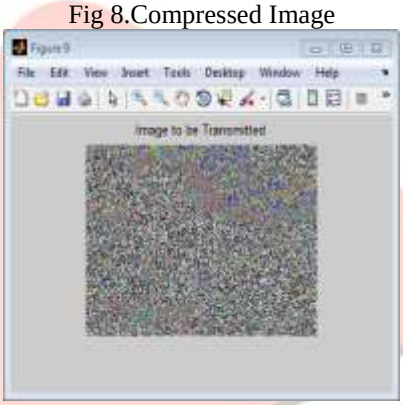

Fig 9.Image to Transmitted

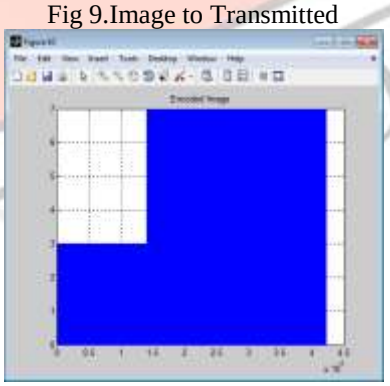

Fig 10.Encoded Image

Fig 11.Decoded Image

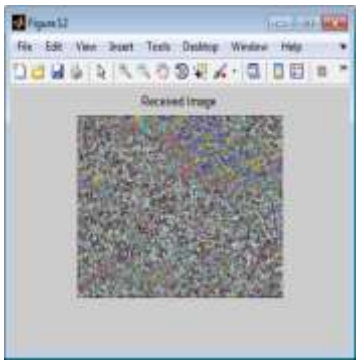

Fig 12.Received Image

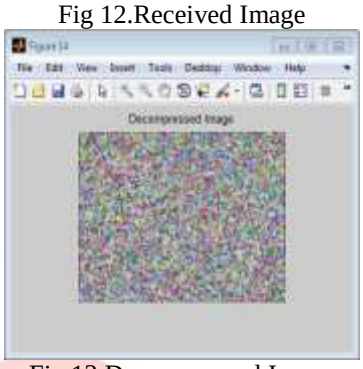

Fig 13.Decompressed Image

Fig 14.Decrypted Image

Fig 15.Extracted Image

4. CONCLUSION

The novel hybrid algorithms are implemented with SDC accomplished in this work, has performed image hiding, encryption, compression and long distance communication efficiently. The hybrid algorithms are categorized and analyzed with reference to the performance evaluation parameters. The parameters show that privacy and security concerns in the secure data transmission could be addressed well.

REFERENCES

[1] Nikolaos G. Bourbakis, — Image Data Compression Encryption Using G-Scan Patterns‖IEEE0-7803-4053-1/97,pp.117-1120,1997

[2] S.S.Maniccam, and N.G.Bourbakis SCAN Based Lossless Image Compression and Encryption IEEE 0-7695-0446-9/99, pp. 490-

499, 1999

[3] Howard Cheng and Xiaobo Li, ―Partial Encryption of Compressed Images and Images‖ IEEE Transactions On Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000

[4] Ebru Celikel and Mehmet Emin Dalkilic, ―Experiments on A Secure Compression Algorithm, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), 2004

[5] Masanori Ito, Noboru Ohnishi, Ayman Alfalou and Ali Mansour, New Image Encryption And Compression Method Based On Independent Component Analysis‖, IEEE, 2007

[6] Younggap You,Hanbyeori Kim,―propose Endoscopy Image Compression and Encryption under Fault Tolerant Ubiquitous Environment 978-1- 4244-4918-7 IEEE, pp. 165-168, 2009

[7] D. Maheswari, V.Radha,―Secure Layer Based Compound Image Compression using XML Compression technique‖ 978-1-4244-5967-4/IEEE,2010

[8] A. Alfalou C. Brosseau, N. Abdallah, and M. Jridi, ―Simultaneous fusion, compression, and encryption of multiple images‖, OPTICS EXPRESS 24024Vol. 19, No. 24 OSA, 2011