International Journal of Research in Advent Technology, Vol.6, No.8, August 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

Trustworthy Media Communications in the IoT by SBPG: Secure Better Portable Graphics

Dr. Shubhangi D.C[1]

Head of the Department of Computer Science &Engg, Visvesvaraya Technological University, Karnataka, India.
DrshubhangiPatil1972@gmail.com

Rumana Ambreen[2]

Department of Computer Science & Engg,, Visvesvaraya Technological University, Karnataka, India.
rumanaambreen786@gmail.com

Abstract-This paper includes the consequences which lies in the IoT environment, specifically Secure mean of communication and user authentication are performed in biomedical images. Exchange of results and data takes place in a smart healthcare environment. A secure camera along with SBPG Compression technique is proposed here. The SBPG architecture includes both encryption and watermarking which overcome all security related issues. The Encryption along with secure blind watermarking technique is used to provide high security with authentic data communication. The resulting data shows that the new BPG compression technique presents high first-rate photograph with authentic information as compare to JPEG approach. The performance of BPG Compression technique has been reached by placing the signature with encryption at middle location of the image and by introducing DCT technique of length 8*8 pixel used by frequency domain blind watermarking technique.

Keywords- Smart Healthcare, Internet of Things (IoT),Secure Digital Camera, Image Communications, Advance JPEG.

1. INTRODUCTION

Medicinal services addresses to be an undeniable with the most appealing solicitation zone for the IoT.As appeared in Fig.1 healthcare monitoring via IoT from remote place.To offer appropriate constant patient information to bliss maintain constrain, which may live in demanding work environments, specialist's pleasantries or over somewhat therapeutic focus, in a related metropolitan or at an assortment of city networks, a brilliant specialist's capacity may utilize spread register and immense data examination. All in all nation, and in tally it make country whereby demanding dominance isn't reliably reachable. The IoT premise relies upon quick letters among the extensive variety of kind of sensors, contraption, and application; on position wellbeing.

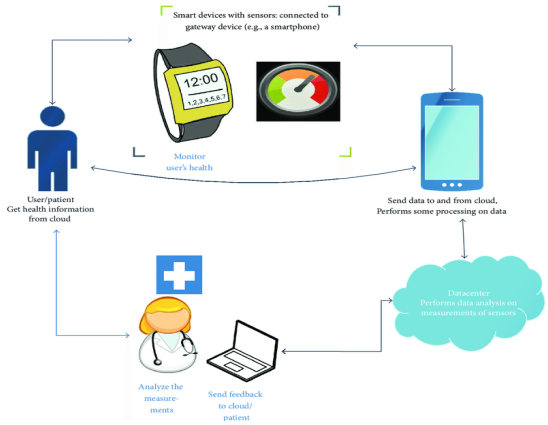


Fig.1 IoT based healthcare monitoring systems

A helpful routine with regards to the IoT when all is accepted in done, and of shrewd medicinal services particularly, speaks to a couple of trouble, tallying vitality capacity of the part associated with the structure; wellbeing of exchange; novel ID of clients that guarantee the security of the clients information; computational usage, unfaltering quality, and adaptability of the structure; fruitful request of expansive datasets bit by bit; and overseeing and put missing colossal occasions of in succession for track-up consider and for training revelation in meta-test arrange. These fundamental nuts and bolts of such systems control colossal trouble on the devices readiness of electronic circuit and structures similar to fearless worth and security. A protected association must to approve the specific identifiable proof of the begin place of data, ensure the profound quality of the data, monitor close to debasement, and should comparatively put contact benefit in this way to the legitimate proprietor of the in succession for help withdrew request and patient succeeding meet-ups.

2. RELATED WORK

Here, a novel, IoT-conscious, SHS architecture for automated monitoring and monitoring of sufferers, personnel, and biomedical gadgets inside hospitals and nursing institutes has been proposed by L. Catarinucci et al[1], With the IoT vision in mind, a complex network infrastructure counting on a CoAP, 6LoWPAN, and REST paradigms has been carried out in order to allow the interoperation among UHF RFID Gen2, WSN, and smart cellular technology.To

securely transfer photo and video records, the quodrotor structure is equipped with an on-board comfy virtual digicam (SDC) proposed by E. Kougianos et al[2] . In such an state of affairs, the quodrotor can be deployed to capture and transmit sensitive records reliably thru using its on-board SDC. This is particularly essential in certain applications where in a 3rd celebration can tamper with the data transmitted from the quodrotor.A general fashion in IWMDs is toward improved functional complexity, software program programmability, and wi-fi network connectivity. An undesirable, yet inevitable, aspect effect of those tendencies is that IWMDs and BANs are an increasing number of vulnerable to protection assaults by Zhang et al [3]. The major goal of a smart town is to decorate the first-rate of offerings furnished to residents to enhance their satisfactory of lifestyles. However, making sure safety and privacy are widespread demanding situations for our future cities can b achieved that is been developed by R. Khatoun and S. Zeadally, et al[4]

Here, EC-based totally signcryption has been used to defend facts captured by clever cameras for event-induced monitoring in IoT packages. They first recognized the capacity threats for such packages and then analyzed decided on security issues. The proposed signcryption, that is implemented at the sensing unit, gives countermeasures to the possible threats and permits the authenticity of encrypted snap shots on the untrusted camera host part without compromising its confidentiality by Ullah, et al[5].The proposed architecture is a unique idea in its domain. Though the consequences are shown handiest for pix, it is able to be easily prolonged for different forms of multimedia. The improvement of a parallel, pipelined, low strength architecture is under progress and could seem in a longer model of the paper by S. P. Mohanty, et al[6].

They have provided a DCT-based totally blind watermarking structures with ultimate watermark coefficients and TSDA (Two Step Detection Algorithm with the aid of EWBHT). The watermark gain, a, is optimized in robustness, invisibility, and capability. They extract a watermark advantage, a, thinking about that BER is less than 20%, MPSNR is extra than 43dB (or PSNR is extra than 38&), and C(Capacity) is half of of the overall capacity of image. This surest watermark advantage, a, enhance the overall performance of watermark structures by B. C. Choi and D. I. Seo, et al[7].

Here, a hardware structure to perform BPG compression encoder in images is offered. The encoding scheme can be divided into two levels. First is the initialization phase, which reads an image and extracts its info then verifies specific parameters along with bit depth, alpha, and colour area. The 2nd segment is HEVC encoding, which is taken into consideration a prime increase in compression strategies.The experimental effects are compared with current JPEG strategies in phrases of excellent and length and suggest the superior compression traits of BPG proposed by U. Albalawi, et al[8].The emerging HEVC widespread has been advanced and standardized collaboratively by means of each the ITU-T VCEG and ISO/IEC MPEG organizations. HEVC represents some of advances in video coding era. Its video codinglayer layout is based on conventional block-based totally motion compensated hybrid video coding principles, but with somecritical differences relative to earlier requirements.When used properly collectively, the functions of the brand new design offer about a 50% bit-price savings for equivalent perceptual pleasant relative to the performance of earlier standards (mainly for a high-resolution video) by G. J. Sullivan, et al[9].

Dual voltage, clock gating and dual frequency techniques were used on this layout for low strength optimization along side with a certain degree of pipelining and parallelism. The structure developed on this layout is the first such architecture so as to carry out both seen and invisible watermarking by] S. P. Mohanty, et al[10]. Here,an electricity-green structure to perform cozy BPG compression encoding is proposed as a built-infeature in a secure virtual digital camera (SDC), which is appropriate for photograph communications within the Internet of Things (IoT) by U. Albalawi, et al[11].

3. IMPLEMENTATION

A. System Architecture

The design arrangement strategy is worried about working up a central fundamental framework for a structure. It incorporates perceiving the genuine parts of the system and exchanges between these sections. The starting design methodology of perceiving these subsystems and working up a structure for subsystem control and correspondence is called development displaying plot and the yield of this blueprint strategy is a depiction of the item auxiliary arranging. The proposed engineering for this framework is given beneath. It demonstrates the way this framework is planned and brief working of the framework.

B. Modules

1. Data Encryption:

AES Algorithm is used as to perform encryption for secure communication. The double layer of assurance in the future design are imperceptible vigorous visually impaired watermarking and AES encryption. Two layers of security are required in light of the fact that all issues recognized with DRM can't be handle through either the watermarking calculations or encryption only. For occurrence, an encryption

calculation anticipates unapproved access of the advanced substance, yet not unlawful

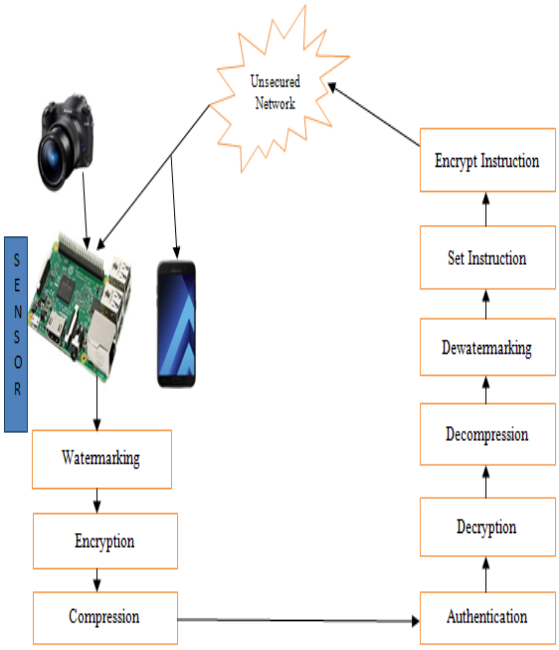


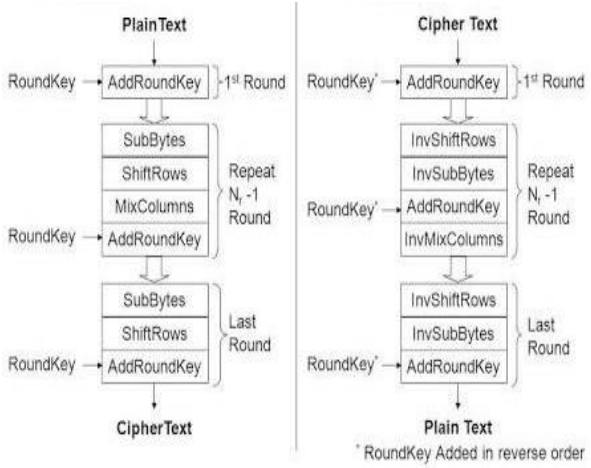
Fig.2 System architecture

duplication of the content has been decrypted via an unapproved client. It can be handle via computerized watermarking.The average structure of AES may be seen in Fig.3.The enter is a single 128 bit block both for decryption and encryption and is referred to as the in matrix. This block is copied into a nation array which is modified at each level of the set of rules and then copied to an output matrix.Both the plaintext and key are depicted as a 128 bit square matrix of bytes. This secret's then improved into an array of key agenda phrases (the w matrix). It need to be mentioned that the ordering of bytes within the in matrix is by way of column. The same applies to the w matrix.

2. Watermarking:

Digital Watermarking: A digital watermark is a variety. of indicator furtively installed in a turmoil tolerant flag, for instance ,sound, video or picture information. It is usually used to discriminate fidelity for copyright of such flag: the clocked data should ,nevertheless does not have to, enfold a link to the carrier flag. Digital watermarks might be operated to corroborate the validation or decorum of the bearer flag or to show the personality of its administration. It is conspicuously utilized for subsequent copyright encroachments and for banknote authentication.

Blind Watermarking: An untraceable vigorous blind watermarking move toward is utilized as a part of conjunction with the Rijndael propelled encryption standard (AES) in the proposed SBPG module.A schematic evaluate of the proposed watermarking algorithm is shown in Fig.4. The host coloration photo is first transformed to YCbCr color space from RGB. The real processing isfinished simplest at the luminance (Y) issue. From this Y aspect of the photograph, the center area of the picture, in which the watermark might be embedded, is extracted. The motivation at the back of the use of the middle zone of the host image for watermark placement is because of reduced computation load and expanded robustness requirements. A pseudo-random wide variety sequence with zero mean and unit variance is used as the watermark within the host image. After placing the watermark within the host photograph, the Cb and Cr additives are introduced to the processed Y issue for that reason generating the very last watermarked colour photo.



Encryption Decryption

Fig.3 AES Algorithm

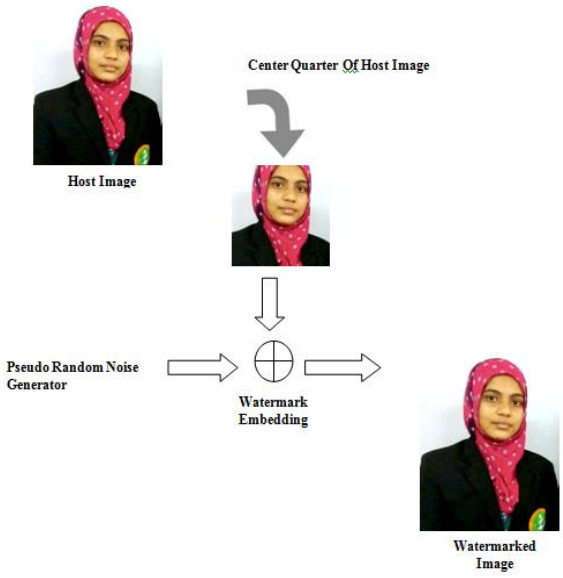


Fig.4 Schematic overview of the proposed watermarking scheme

2.1. Insertion Algorithm

Watermarking embedding is completed on a shade image of size N*N .As a first step of embedding, the color photo is converted from the RBG area to the YCbCr area and handiest the Y element is considered for further processing. The Y picture aspect is split into an equal number of 8*8 blocks and DCT is accomplished on each block. Since the middle part of the picture is the focus of interest from the viewers' point of view, the watermark might be embedded in the center region of the photograph.

The selection of suitable DCT coefficients for watermarking is very important. The low frequency coefficients contain much of the signal energy, and the human eye is also more sensitive to these frequencies as compared to high frequency coefficients. On the other hand, the high frequency coefficients contain edge information and details. Any change in low frequency coefficients due to watermarking may degrade the quality of the image and the watermark implemented in high frequency coefficients may be easily altered by attacks (intentional or unintentional) such as data compression, low pass filtering, and sub-sampling. Hence, it is best to select mid frequencies for watermark insertion to maintain the robust-ness to attacks and the quality of the watermarked image. Keeping this in mind, four mid-frequency coefficients are chosen as $C_{4;1}$, $C_{3;2}$, $C_{2;3}$, and $C_{1;4}$ (in Fig.5 they are labeled 19, 18, 17 and 16) from each block in the center quarter of the image. Through these coefficients, a vector Q of size N is generated where P is the number of 8*8 blocks in the center quarter of the image:

$Q = \{r_{1,i}, r_{2,i}, r_{3,i}, r_{4,i}, \ldots, r_1, N, r_2, N, r_3, N, \ldots, r_4, N\}$, (1)

where $r_{x;y}$ is the coefficient of the selected block y.

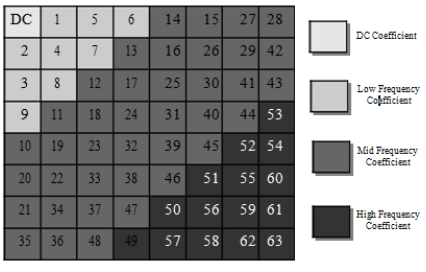


Fig.5 DCT coefficient numbering scheme for an 8*8 block.

A pseudo random sequence is chosen from 1000 pseudo random sequences of size 4 N and is then used as the watermark represented as:

$B=\{a_1, a_2, a_3, \ldots, a_{4\times N}\}$, (2)

where every element is of zero mean and unit variance. The watermark B is to be embedded into the DCT coefficients of the image of vector R according to:

$$r_i' = r_i + \alpha |r_i| a_i, \quad (3)$$

for i = 1,2,,, 4*N and is a scaling constant, which is used to determine the watermark strength.Small values of α could make the watermark vulnerable to modification and also make it difficult to extract and detect in the course of the detection/extraction level. Similarly, huge values of α could make the watermark visible. So an choicest desire of this scaling regular is important.This process forms a new vector Q' given by:

$$Q' = \{r_1', r_2', r_3', \ldots, r_{4\times N}'\}, \quad (4)$$

That's of the equal size as vector Q. These new values of Q are reinserted into the DCT coefficients of the corresponding blocks, and then the block-clever inverse discrete cosine transform (IDCT) is carried out. This offers the changed Y' issue in the spatial area. The Cb and Cr additives of the host photo are then concatenated with y' which will gain the colour photograph. This image is finally transformed to the RGB area, and the ensuing photo is the watermarked photograph, O' . The complete embedding and detection insertion method is shown in Fig.7.

The embedding process of the binary watermark image into the host image is presented in this sub-section. The host image's size should be dyadic (2^nx2^n) and a binary image is used as watermark. Initially, the non-overlapping blocks of size 2x2 are extracted from the host image. A pixel of binary watermark image is embedded into a single block. The mean calculation, embedding strength (γ) and signum function are employed in the process of embedding the watermark. Originally, each non-overlapping block is converted into a vector, and the mean value of the vector is computed. Afterwards, the mean value is divided by the embedding strength (γ) and used in the embedding. As the watermark is a binary image, the embedding of watermark involves two cases: embedding pixel value '1' and embedding pixel value '0'. Two distinct mathematical operations are performed for embedding pixel value '0' and '1'. Fig.6 shows the block diagram of the watermark embedding process.

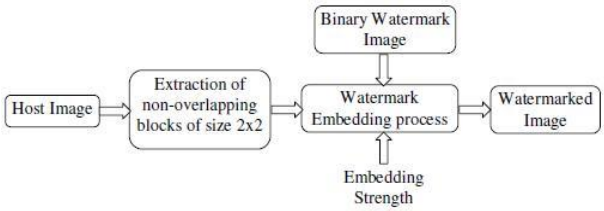


Fig.6 Watermark Insertion Process

Watermark Insertion Steps:

Input: Host Image (I), Binary Watermark Image (W),

Embedding strength (γ)

Output: Watermarked Image (I_W)

1. The binary watermark image (W) of size n x n consists of n^2 number of pixels. Extract n^2 number of 2x2 non-overlapping blocks from the host image. The extracted non-overlapping blocks are stored in a vector B.
$$B = [b_1, b_2, b_3, ..., b_N]\ ;\ where\ 0 < N \leq n^2$$
2. Convert each matrix in the vector B into a vector V_B.
$$V_B = [x_1, x_2, x_3, x_4]$$
3. Calculate the mean value for all the converted vectors V_B.
$$\bar{V}_B = \frac{\sum_{i=1}^{k} V_{B_k}}{k}\ where\ 0 < k \leq 4$$
4. Divide the mean value V_B of all the vectors by embedding strength γ and denote the resultant value as Q.
$$Q = \frac{\bar{V}}{\gamma^B}\ ; where\ \gamma = 2$$
5. The binary watermark image pixels are embedded into the blocks in vector B using the predetermined Q and embedding strength γ as follows:
   (i) Calculate the signum function of each block in vector B and store it in another vector X. The signum function is the real valued function defined for real x as follows [24]
$$sgn(x) = \begin{cases} +1, & if\ x > 0, \\ 0, & if\ x = 0, \\ -1, & if\ x < 0. \end{cases}$$
   For all real x we have sgn(-x) = -sgn(x). Similarly $|x| = sgn(x)x$. If $x \neq 0$ then also
$$\frac{d}{dx}|x| = sgn(x).$$
   The second property implies that for real non-zero x we have $sgn(x) = x/|x|$
   (ii) For pixel value '0' perform the following mathematical operation
$$t = ((round\ (Q * 0.5) * 2) * \gamma)$$
   (iii) For pixel value '1' the following mathematical operation is carried out.
$$Q_t = (Q - 1)$$
$$t = ((round\ (Q_t * 0.5) * 3) * \gamma))$$
   (iv) Multiply each block in vector X by the calculated value t with respect to watermark pixel and place it in vector B.
$$B << (X_{(i)} .* t)\ ;\ where\ 0 < i \leq k$$
6. Map the modified blocks in the vector B back to its original position in host image I to obtain the watermarked image I_W.

2.2. Detection Algorithm

The essence of the blind set of rules is the non-availability of original picture facts at the detector aspect.During the watermarking system, the authentic Y'CbCr has been transformed to YCbCr. There can be some corruption, noise, and distortion that could appear to the watermarked photograph due to transmission, attacks, and processing of the photo. So this Y'CbCr picture (or O') is modified to image YCbCr (or O). The DCT of O is then taken in a block-through-block manner where the block length is 8. The principal sector of the photograph is diagnosed which will extract the coefficients from which the watermark will be extracted. The same mid frequency coefficients should be selected that have been considered within the watermark insertion system, as these sets of coefficients provide information approximately the presence of watermark. From the selected coefficients, a vector Q of size 4 N is generated if you want to provide information:

$$Q = \{r_1^*, r_2^*, r_3^*, \ldots, r_{4\times N}^*\}. \quad (5)$$

To decide the presence of a watermark in picture O , a correlation coefficient is derived consistent with the watermark B, which is inserted into the DCT coefficient of the photograph of vector Q in Eqn. 3. The correlation coefficient is defined to compute the correlation between the extracted coefficients Q and the watermark B itself the usage of the formula:

$$\sigma = \frac{BQ^*}{N} = \sum_{i=1}^{N} a_i r_i^*. \quad (6)$$

The ideal situation where the watermark is not corrupted occurs when:

$$r_i^* = r_i' = r_i + a|r_i|x_{i,} \quad (7)$$

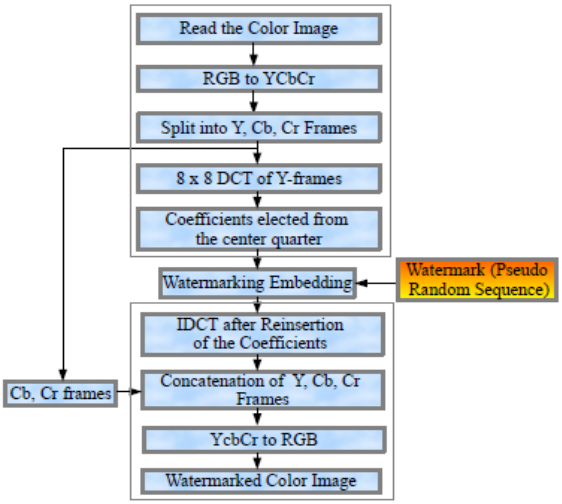


Fig.7 Insertion Algorithm

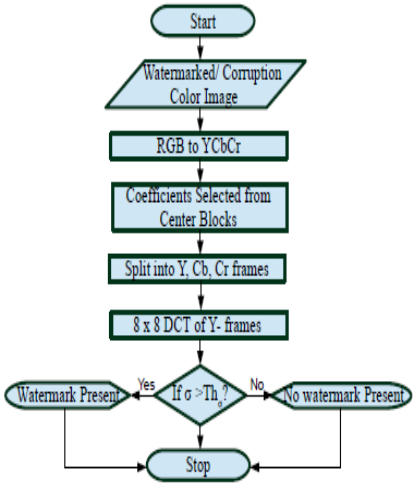


Fig.8 Detection Algorithm

where X is the vector of DCT coefficients. In that case, the correlation will be:

$$\sigma = \frac{1}{N} = \sum_{i=1}^{N} r_i a_i + \alpha |r_i| x_i a_i. \qquad (8)$$

When B and X are matched the correlation will be:

$$\sigma = \frac{1}{N} = \sum_{i=1}^{N} r_i a_i + \alpha |r_i| a_i^2. \qquad (9)$$

Assuming zero means of the vectors r_i's and x_i's,μ equals $\alpha\mu_{|r|}$when B = X; otherwise,μ equals 0.A threshold Th_σ is described in order that through evaluating the calculated σ with this threshold Th_σ , it's far viable to decide the presence or absence of a watermark. In order to test the robustness of the proposed set of rules and growth the edge, different values of threshold are selected. Starting from the price 2.0, an ordeal and error approach become observed by using attempting values of 1.8, 1.6, 1.4, 1.2, 1.0, and 0.8. The fee 1.2 gives the great outcomes over all take a look at pics taken into consideration.. This threshold is determined the usage of the following expression

$$Th_\sigma = \frac{\alpha}{1.2N} \sum_{i=1}^{N} |r_i^*| \qquad (10)$$

The decision is made based on the following: If σ >Th then a watermark is gift and if σ <Th then a watermark is absent. This helps to make decisions about the authenticity of the photograph. The normal algorithm float for watermark detection is provided in Fig.8.

2.3. Watermark Extraction Algorithm

The extraction of binary watermark picture from the watermarked photograph is explained in this sub-section as shown in Fig.9. As the proposed scheme is blind, the extraction calls for: watermarked picture, size of watermark photograph, embedding energy and it doesn't require the authentic picture or any of its characteristics. To start with, 2x2 non overlapping blocks are extracted from the watermarked picture and the variety of blocks extracted depends on the dimensions of the watermark image. The blocks for this reason extracted are stored in a vector. Afterwards all the extracted blocks are transformed into a vector and the mean value of the vector is calculated. Subsequently the imply values of all the blocks are divided with the aid of the embedding electricity. The resultant price is applied within the extraction of watermark. Finally, a matrix with length of watermark image is initialized and the extracted pixel values are positioned in it in an effort to gain the watermark photo.

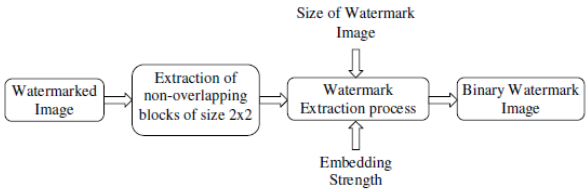


Fig.9 Watermark Extraction Process

Input: Watermarked Image (I_W), Size of watermark image (W) , Embedding strength (γ)
Output: Watermark Image (W)

1. Extract 2x2 non-overlapping blocks from the watermarked image (I_W). The number of extracted blocks should be equivalent to the size of watermark image. Store the extracted blocks in a vector BV .
   $BV = [b_1, b_2, b_3, ..., b_N]$; *where* $0 < N \leq n^2$
2. Convert each block in the vector BV into a vector V_B .
   $V_B = [x_1, x_2, x_3, x_4]$
3. Calculate the mean value of all the converted

vectors $\overline{V_B} = \frac{\sum_{i=0}^{k} V_{B_k}}{k}; where\ 0 < k < 4$

4. Divide the calculated mean value $\bar{V}_B$ of all the vectors by the embedding strength γ . The value thus resulting is denoted as Y .

$Y = (\overline{V_B} / \gamma)$; *where* $\gamma = 2$

5. Perform the following mathematical operation and store the result in a vectorW_p .

W_p << $(Y[i] \bmod 2)$; $0 \le i \le |W|$

6. Initialize a matrix with size of watermark image and place the extracted pixel values (W_p) in it to

obtain the watermark image (W) .

3. Compression

The SBPG module plays out the BPG compression, yields higher compression amount analyzed JPEG pictures without trading off the decompressed picture clearance.Carrying watermarking and information encryption before BPG compression is more secure method contrasted with the turnaround approach in light of the fact that watermarking after compression implies watermarking in light of changed data of the crowd picture.

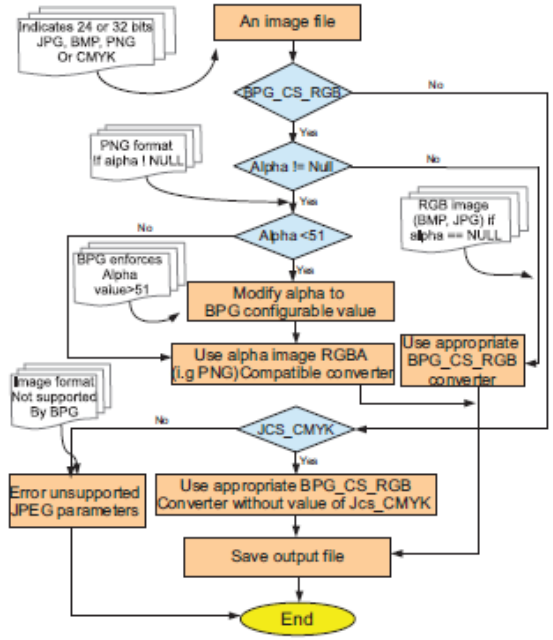


Fig.10 BPG Encoder Algorithm

After reading the image as shown in Fig.10, the encoder does initialization processes to read meta data, color space, bit depth, etc. There is an essential step in which the algorithm must check two conditions: bit depth and color space. Bit (color) depth refers to the amount of data that can be used to indicate the color of each pixel. It can be represented by different numbers: 8,10, 12,…… It describes the number of bits used to represent colors per pixel. The concern with images that have high bit depths are data storage, and required transmission bandwidth.Also, some displays are not capable of reproducing all of these colors. Undoubtedly, there must be a trade off between quality and bit depth. The BPG compression encoder strictly considers images with bit depth of 8.

4. RESULT AND DISCUSSION

RMSE compares the extracted watermark O to that of the stored original image O of size m n and is given by the following expression:

$$RMSE=\frac{1}{\sqrt{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N=1} \| \left(o(i,j) - o'(i,j)\right) \|^2 \quad (11)$$

PSNR is the ratio between the maximum possible energy of O (E_{max}) and the power of the corrupted image O' from watermarking and is given by the following expression:

$$PSNR = 20 \log\left(\frac{E_{max}}{MSE}\right) \quad (12)$$

It can be seen from the re sults that the visual quality of the image is maintained so that the change in the image quality before and after watermarking cannot be perceived by the human eye. Selected results are presented in Fig.11.

(a) Cover Image (b) Watermarked (= 0:2)
(c) Watermarked(=0:65)

Fig.11 Watermarking of "Image" (256 256).

Comparison with prior works

There is a good sized body of literature available on watermarking. This subsection gives a evaluation of the proposed watermarking insertion set of rules to other currently used algorithms. The consequences ares shown in Table 1. As may be seen from the Table, the proposed set of rules gives higher PSNR while there are no assaults at the watermarked snap shots. From the preceding results, it additionally exhibits that the proposed watermark set of rules is strong to most photo attacks, consisting of noise.

Table 1 PSNR values for different watermarking algorithm.

S. No.	Algorithm	PSNR

1	Image adaptive watermarking	40.054 dB
2	Image adaptive watermarking creation	45 dB
3	Zerotree of wavelet	44.18 dB
4	9/7 biorthogonal wavelet lifting	36.44 dB
5	Robustness of DCT-based watermarking against JPEG compression	34 dB
6	DCT-based watermarking using inter-block coefficient correlation	41.78 dB
7	Metric-based fitness function for robust watermarking	> 41.63 dB
8	Proposed Algorithm	> 41.81 dB (in case of code simulation) > 44.37 dB (in case of Simulink® model)

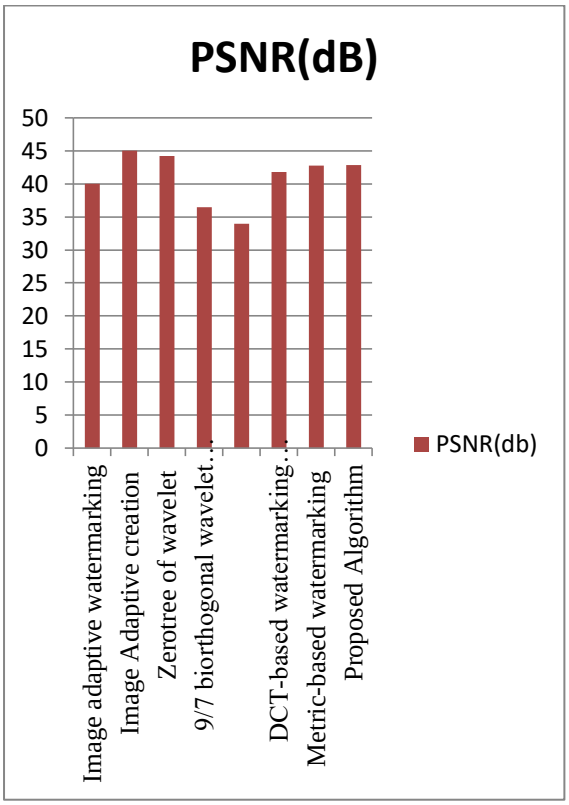


Fig.12 Comparison of different algorithm based on PSNR

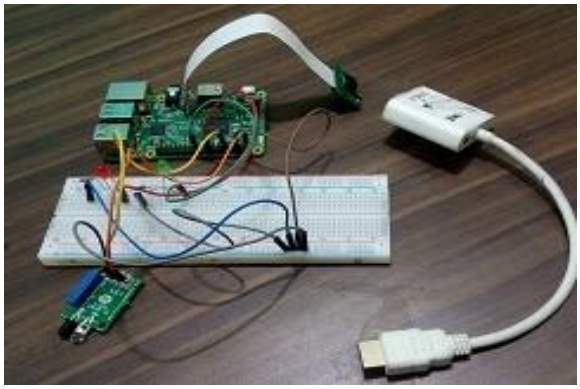


Fig.13 Hardware Components

Fig.14 Home page

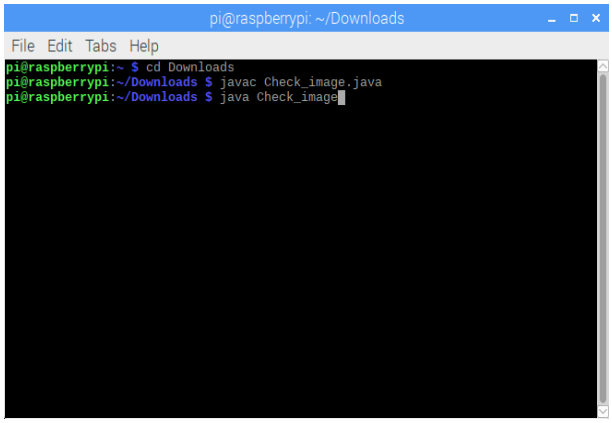


Fig.15 Checking image on client side

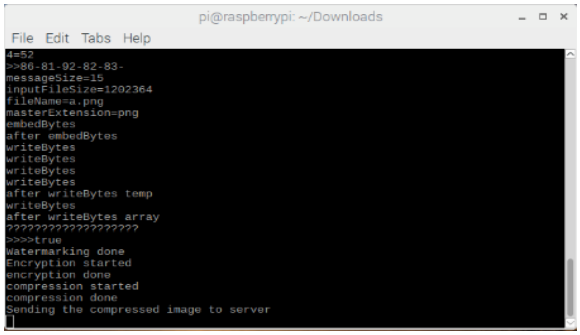


Fig.16 Performing Encryption, Compression Watermarking on client side

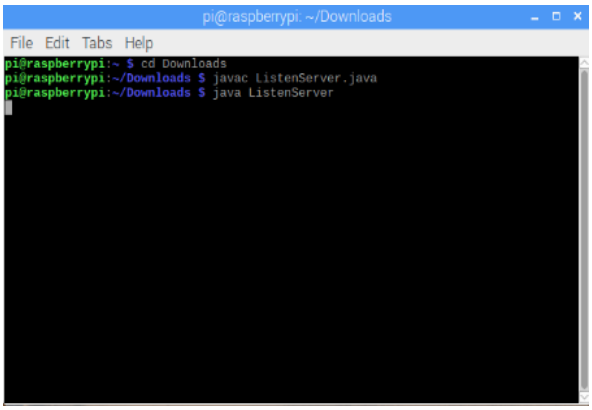


Fig.17 Client Listening Server

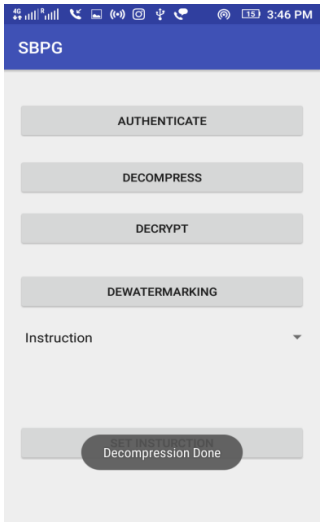


Fig.18 Decompression done on server side

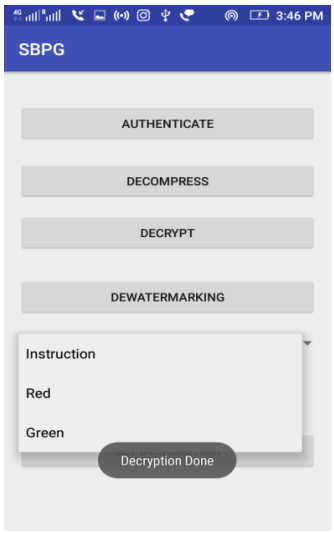


Fig.19 Decryption done on server side

Fig.20 Dewatermarking done server side

Fig 15 & 16 shows the encryption ,watermarking and compression performed on an image containing the authentic information or an message that needs to be send to the server/doctor more securely.Fig.17 represent the client listening the the response from server after sending the image.

The image received from client/patient will be decompressed, then decrypted on server side. Finally the image is dewatermarked as shown in Fig 18,19 & 20 and based on the content of the image appropriate instructions will be send on patient/client side based on which the patient will be treated.

5. CONCLUSION

This paper consists of the effects which reside inside the IoT surroundings, particularly Secure reliable communication of verbal data and consumer authentication are established in biomedical images. Sharing of data and results take place in a secure healthcare environment. A comfortable secure camera along with BPG Compression Algorithm are proposed in SBPG architecture. The SBPG architecture consists of each encryption and watermarking techniques which overcome all safety related troubles from existing JPEG approach. The Encryption along with a secure blind watermarking approach is used to offer high protection. The resulting outcomes shows that the new BPG compression technique presents high first-rate photograph with authentic information as compare to JPEG approach. Thus the performance of BPG Compression method has been improved by adding encrypted signature at the central part of the image and through introducing DCT approach of 8*8 pixel utilized by frequency domain watermarking approach.Therefore, based on the analysis of result,the proposed Advanced JPEG technique along with blind watermarking approach reduces the processing

complexity and provides well security with realiable mean of communication by proposing.

REFERENCES

[1] L. Catarinucci*et al.*, ``An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515 526, Dec. 2015.

[2] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, ``Design of a high-performance system for secure image communication in the Internet of Things," *IEEE Access*, vol. 4,pp.1222 1242, 2016.

[3] Zhang, A. Raghunathan, and N. K. Jha, ``Trustworthiness of med-ical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8,pp. 1174 1188, Aug. 2014.

[4] R. Khatoun and S. Zeadally, ``Cybersecurity and privacy solutions in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 51 59, Mar. 2017

[5] Ullah, B. Rinner, and L. Marcenaro, ``Smart cameras with onboard sign-cryption for securing IoT applications," in *Proc. Global Internet ThingsSummit (GIoTS)*, 2017, pp. 1 6.

[6] S. P. Mohanty, N. Pati, and E. Kougianos, ``A watermarking co-processor for new generation graphics processing units," in *Proc. 25th IEEE Int.Conf. Consum. Electron.(ICCE)*, Jan. 2007, pp. 303 304.

[7] B. C. Choi and D. I. Seo, ``A statistical approach for optimal water-mark coefcients extraction in HVS-based blind watermarking system," in *Proc. 7th Int. Conf. Adv. Commun. Technol. (ICACT)*, vol. 2. 2005,pp.1085 1088.

[8] U. Albalawi, S. P. Mohanty, and E. Kougianos, ``A hardware architecture for better portable graphics (BPG) compression encoder," in *Proc. 1stIEEE Int. Symp. Nanoelectronic Inf. Syst.*, Dec. 2015, pp. 291 296.

[9] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, ``Overview of the high efciency video coding (HEVC) standard," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 22, no. 12, pp. 1649 1668, Dec. 2012.

[10] S. P. Mohanty, N. Ranganathan, and K. Balakrishnan, ``Design of a low power image watermarking encoder using dual voltage and frequency," in *Proc. 18th Int. Conf. VLSI Design*, 2005, pp. 153 158.

[11] U. Albalawi, S. P. Mohanty, and E. Kougianos, ``Energy-efcient design of the secure better portable graphics compression architecture for trusted image communication in the IoT," in *Proc. IEEE Comput. Soc. Annu.Symp. VLSI (ISVLSI)*, Jul. 2016, pp. 302 307.

[12] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart Cities: A Survey on Data Management, Security and Enabling Technologies," IEEECommunications Surveys Tutorials, vol. PP, no. 99, pp. 1–1, 2017.

[13] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities," IEEE Consumer ElectronicsMagazine,vol. 5, no. 3, pp. 60–70, July 2016.

[14] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care," IEEE Consumer Electronics Magazine, vol. 8, no. 1, pp. x–y, Jan 2018.

[15] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515–526, Dec 2015.

[16] F. Bellard, "The BPG Image Format," http://bellard.org/bpg/, last Accessed on 09/20/2015.

[17] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things," IEEE Access, vol. 4, pp. 1222–1242, 2016.

[18] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of Medical Devices and Body Area Networks," Proceedings of the IEEE, vol. 102, no. 8, pp. 1174–1188, Aug 2014.

[19] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System," in Proceedings of the 13th IEEE International Conference on e-Health Networking, Applications and Services, 2011, pp. 150–156.

[20] R. Khatoun and S. Zeadally, "Cybersecurity and Privacy Solutions in Smart Cities," IEEE Communications Magazine, vol. 55, no. 3, pp. 51– 59, March 2017.