International Journal of Engineering & Technology, 7 (2.20) (2018) 93-96

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Robust and brittle secured video for IOT

K. Lakshmi Narayanan[1*], G.P. Ramesh[2], V. Divya[3]

[1] Research Scholar, Department of E.C.E, St. Peter's Institute of Higher Education and Research, Chennai, India
[2]Professor & Head, Department of E.C.E, St. Peter's Institute of Higher Education and Research, Chennai, India
[3]P.G. Scholar, Francis Xavier Engineering College, Tirunelveli.
**Corresponding author E-mail:kyelyen@gmail.com*

Abstract

In this paper the system is mainly designed for the military purpose security since now-a-days securing our military has become a difficult task .our live is mainly dependent on other objects mainly we are computer based living and digital image processing plays a vital role in it. This process has much advantage as well as some disadvantage. A VLSI circuit is built with many millions of IC chip, so it is considered to be indivisible for the construction purpose. The internet-of things (Iot) is a electronic device which is connected to the vehicle and the building item which is used to generate many secured techniques which is connected with the software, electrical, electronics and mechectronics devices and human recourses also. Better Portable Graphics Algorithm with a Context-Adaptive Binary Arithmetic Coding (CABAC) encoding algorithm is used in the existing system this process is affected by the Gaussian noise, low compression ratio and time delay to overcome above issues and enhanced with Secure Better Portable Graphics (SBPG) compression algorithm with HEVC is present .The proposed architecture is suitable for high performance imaging in the Iot and for the high quality compression files and secured transformation of image and video captured in the digital camera. Encryption and watermarking are the two technique used in the process. The watermarking technique is more secure than the previous system. This process produces high quality JPEG, and high PSNR ratio. The scrambling algorithm is used in the encryption process. It is used for providing secured image.

1. Introduction

The process in which the Object recognition method is used for determining the object present in the image or video. It is considered to be a difficult task since the object is detected depending upon various factors like the position of object and object model difference which is relative to the camera and the lighting variation also. Between the frames and the position the desired object can be determined by tracking The efficient and exciting products to market are produced due to the transformative prove of Iot. The Iot is mainly useful for the military purpose for the tracking of people from the outside area entering our area would be founded easily through this process.



Figure 1.1: Internet of things

The vehicles in which the camera is placed, and the quadrator consist of four cameras to view 360 degree so the incident which is happening in the surrounding can be predicted. The Iot is otherwise known as the **smart device** or **connected device.** When the Iot is connected to the sensor it make use of many object..It can be used in the environmental aspects like weather monitoring of the air, water and other natural hazards which are happening in our surrounding.

2. Novel contribution of this paper

The secured better portable graphics algorithm (SBPG) is used for the secured video communication process which can be highly used in the military source and defense. It consists of double layer 1.encryption and 2.watermarking. The process of hiding the data is called the encryption. The robust watermarking is the process used in this System, watermarking is nothing but the process of giving cover image to the system. Brittle is known as the side channel attack, which means the process of giving cover image to the frame ,when the hacking is held the data cannot be changed and the cover image is corrupted and the frame remains same. The SBPG encoding consist of several advantages over JPEG compression including high quality with lower size than JPEG, which makes it suitable for real time applications and bandwidth requirements. The aim of this process is to secure the video\image communication by using internet of things and to overcome

- Low compression ratio.
- Reconstructed image affected by Gaussian noise.
- External disturbance and error.

3. Proposed architecture for SBPG

Image and video compression

The process in which detecting an object is considered to be difficult. The process in which our main aim is to introduce Secured Better Portable Graphics (SBPG)compression algorithm for securing the image/video communication. The system is more over used in the civil application. It is being implemented in the robotics so that it is able to perform a set of task, make a decision on fly and interact with their surroundings. The process can reduce

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the redundancy between the blocks in the HEVC frames. The process in which JPEG achieves higher compression ratio with smaller size.

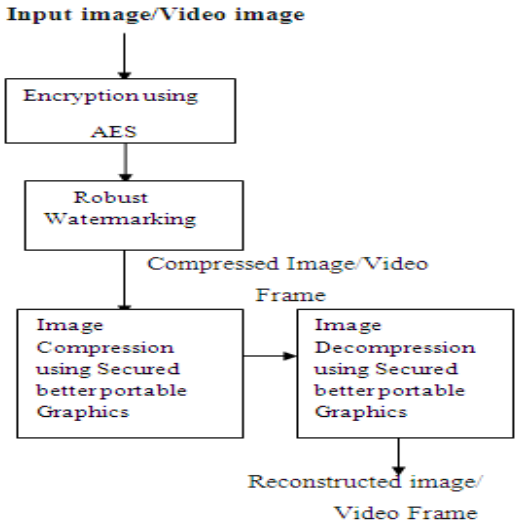


Figure 3.1: Block diagram

Encryption

The conversion of electronic data into another form, and which cannot hypertext and can be easily understood by anyone except authorized parties is called the encryption .The digital data stored on computer system or transmitted via internet or any other computer system is protected by the encryption process. In early time people are not able to read so writing the secret message was enough but the encryption was developed which covert the message to a secret code moreover the contents are reordered or replaced with the help of characters, numbers, symbol etc. In the security of IT system and modern communication the encryption plays a vital role. In the usage of Iot encryption is also used in the military and government for securing communication. In many kind of civilian systems encryption is used for protecting information. The encryption is divided as,

- Symmetric encryption
- Asymmetric encryption.

The early time used method is the symmetric process which uses the letters, characters, symbol etc, which is applied to the message and it is used for securing the data. The major problem occurred in the internet or any other largest network is preceded with the help of asymmetric encryption .The frames of the video are first encrypted and the process takes place.

Scrambling algorithm

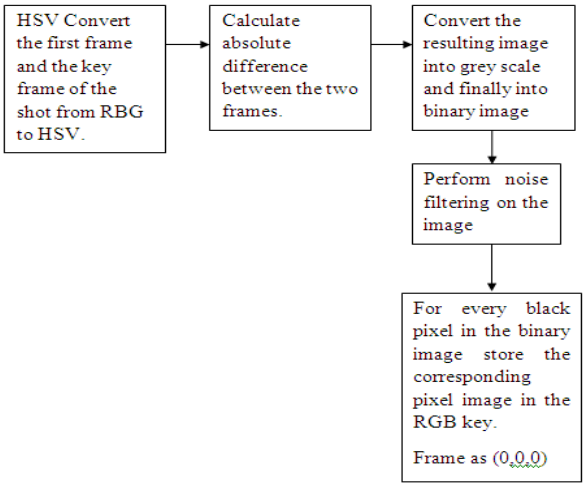


Figure 3.2: Scrambling technique

Video scrambling is mainly used in the encryption system; they are preceded in the binary values. It is used in the broadcasting video streams. The process in which image or video of the first frame and the second frame are compared to find out the absolute different value where the same values are considered till the n^{th} process and the different values are rejected the process is continued till the end of the N number of frames. Noise filter is used in the system so that the distortion can be removed easily. The binary image storage to the corresponding pixel image in the RGB key is also noted.

Watermarking

Robust watermarking is the technique used in this process which is used for the hiding purpose, when it resists a designated class of transformations. The process of hiding digital information in the form of carrier signal is called watermarking, but the carrier signal does not have any contact with the hidden information. The watermarking mainly depends on the use case. Source tracking is considered to be the main application of watermarking. The watermarking is divided as

1. Fragile watermarking
2. Semi-fragile watermarking

The slit change or modification indentified is called fragile watermarking. The interior proof system is used in the fragile watermarking. During the transformation the process which resist is called the semi-fragile watermarking. The watermarking is applicable in copyright, tracking, and broadcast monitor. After the data is encrypted the watermarking is held, which provide a cover image to the frame, so that it cannot be read by the other parties.

Compression

Encoding information using data compression, source coding converts large bits to smaller bits in signal processing. The two types of compression are lossy and lossless compression .The process of eliminating redundancy and identifying bits are called lossless compression. Dropping non essential detail is called lossy compression. After the completion of the encryption and watermarking the compression is held with the help of secured better portable graphics algorithm. When it is compressed the numbers of frames are noted.

Decompression

Source encoding converts smaller bits to larger is called decompression. The opposite process of compression is the decompression. The compressed files are decompressed using the secured better portable graphics algorithm, so the number of frames is converted to the image/ video form.

4. Result and analysis

Encryption using AES

The process of encryption in AES architecture. The process is carried out by the frames from the input video and the key whose size is also 128 bit such as “VLSI”. The encryption process produces the cipher text of 128 bits after 10 rounds of processing, as shown above.

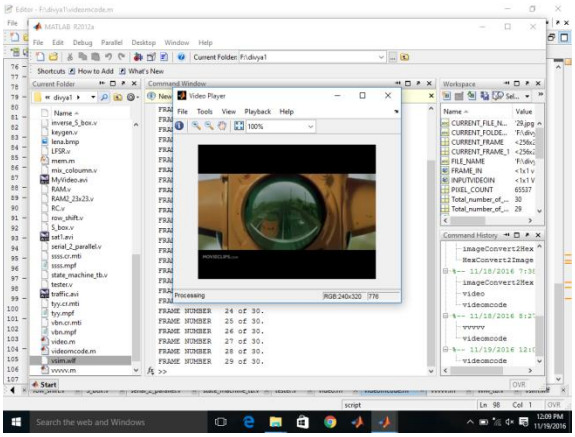


Figure 4.1: Image to text convertor

Figure 4.1 explains the process of image conversion using the encryption method so that the above image will not be corrupted

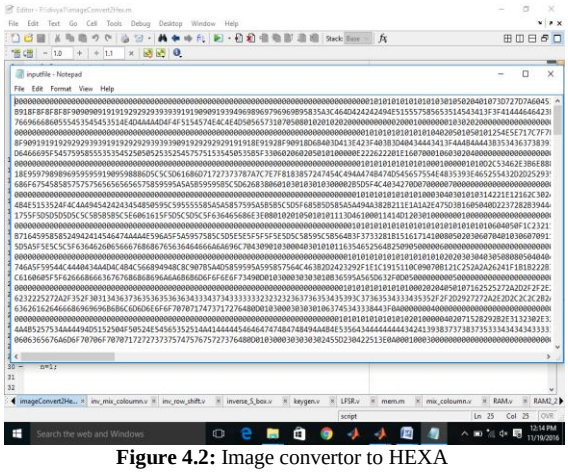


Figure 4.2: Image convertor to HEXA

Figure 4.2 in which the image is converted to the hexa value through which the data cannot be visible. The total number of frames is also converted to the hexa.

Simulation of watermarking

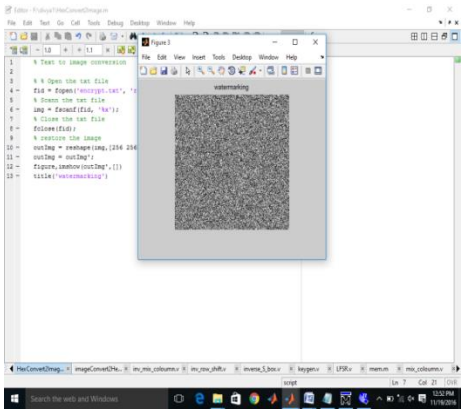


Figure 4.3: Simulation of watermarking

Figure 4.3 in which the watermarking is implemented. The process of providing cover image to the frame, so that it can be easily secured from the side channel attack.

Simulation of AES Decryption

It explains the decrypted file where the frames are then converted to the video using the SBPG algorithm and the values are assigned.

Figure 4.5 represents the block compressor of the system where the blocks are being shown.

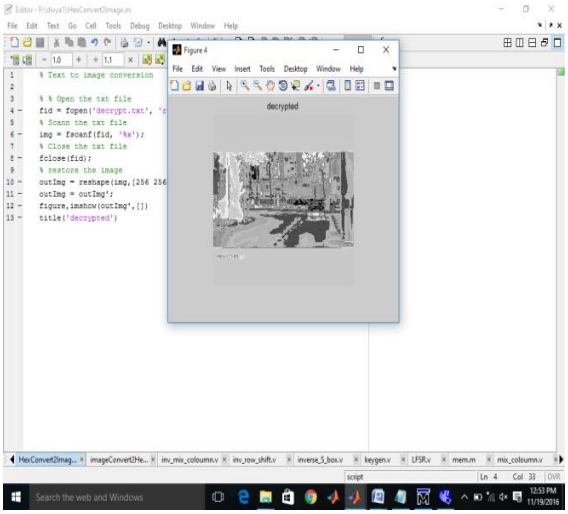


Figure 4.4: Simulation of AES Decryption

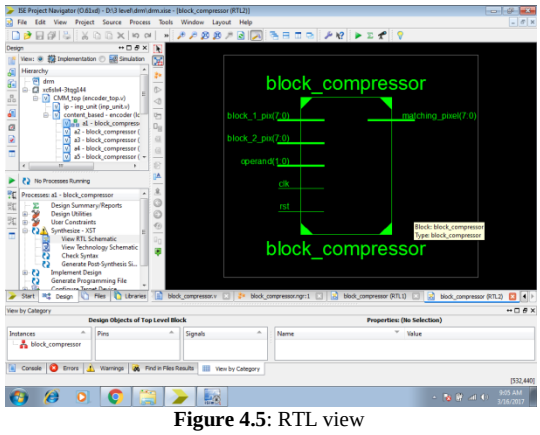


Figure 4.5: RTL view

Schematic representation

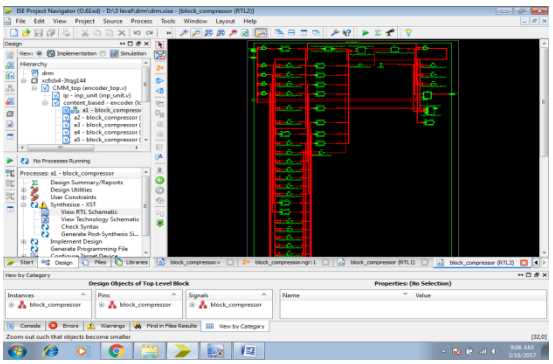


Figure 4.6: Schematic representations

The number of chip used in the system are been represented through this block

5. Conclusion

With the wide use of internet this work is focused to implement the internet technology to establish a system which would communicate through internet for better health. Internet of things is expected to rule the world in various fields but more benefit would be in the field of healthcare. Hence present work is done to design an IOT based secure video communication. In this work, for secure video communication double layer protection scheme is used. Double layer protection means encryption and watermarking are used. For encryption advanced encryption standard is used and robust watermarking is used for watermarking. The data is sent to

the destination via a secure channel. From the experimental results this method provides better security than previous schemes.
In future fragile watermarking is used for improving security of video communications. Fragile watermarks are commonly used for tamper detection (integrity proof). To verify the authenticity or integrity of carrier signal digital watermarking may be used, which is used to identify the tracing copyright.

References

[1] Altu˘g E, Ostrowski JP & Taylor CJ, "Control of a Quadrotor Helicopter Using Dual Camera Visual Feedback", *The International Journal of Robotics Research*, Vol.24, No.5, (2005), pp.329–341.

[2] Coelho G, Kougianos E, Mohanty SP, Sundaravadivel P & Albalawi U, "An IoT-Enabled Modular Quadrotor Architecture for Real-Time Aerial Object Tracking", *Proceedings of the 1st IEEE International Symposium on Nanoelectronic and Information Systems*, (2015), pp.197– 202.

[3] Crespo G, de Rivera GG & Ponticelli R, "Setup of a communication and control systems of a quadrotor type Unmanned Aerial Vehicle", *Proceeding Conference on Design of Circuits and Integrated Circuits (DCIS)*, (2014), pp.1–6.

[4] Hao ND, Mohamed B & Rafaralahy H, "Trajectory-tracking control design for an under-actuated quadrotor", *Proceeding of European Control Conference (ECC)*, (2014), pp.1765–1770.

[5] Liu C, Shen W, Ma T, Fan Y & Zeng X, "A Highly Pipelined VLSI Architecture for All Modes and Block Sizes Intra Prediction in HEVC Encoder", *Proceedings of IEEE 10th International Conference on ASIC (ASICON)*, (2013).

[6] Mody M, Garud H, Nagori S & Mandal DK, "High Throughput VLSI Architecture for HEVC SAO Encoding for Ultra HDTV", *Proceedings of IEEE International Symposium on Circuits and Systems*, (2014).

[7] Mondragón IF, Olivares-Méndez MA, Campoy P, Martínez C & Mejias L, "Unmanned aerial vehicles UAVs attitude, height, motion estimation and control using visual systems", *Autonomous Robots*, Vol.29, No.1,(2010), pp.17-34.

[8] Mohanty, SP Kougianos E, Cai W & Ratnani M, "VLSI Architectures of Perceptual Based Video Watermarking for Real-time Copyright Protection", *Proceedings of the 10th International Symposium on Quality Electronic Design (ISQED)*, (2009), pp.527 –534.

[9] Shoufan A, "A hardware security module for quadrotor communication", *Proceeding International Conference on Field-Programmable Technology (FPT)*, (2012), pp.253–256.

[10] Sullivan GJ, Ohm JR, Han WJ & Wiegand T, "Overview of the High Efficiency Video Coding (HEVC) Standard", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol.22, (2012), pp.1649–1668.