Security of Image for Internet of Things Device (Camera)

[1]R.Ajith Krishna, [2] N. Sharath Kumar, [3]K.Priyanka, [4]Josepha Menandas. J
[1]Third year Student, Dept of ECE, [2]Third year Student, Dept of IT, [3]PG Scholar, Dept of CSE,
[1]College of Engineering, Guindy, Chennai, INDIA,[2]Rajalakshmi Engineering college, Chennai, INDIA
[3]Dept of CSE, Panimalar Engineering college, Chennai, INDIA
[4]Asso.Professor, Dept of CSE, Panimalar Engineering college, Chennai, INDIA.
ajithkrishna1997@hotmail.com, sarathn1997@gmail.com, priyanka.ak24@gmail.com, josepha82@gmail.com

Abstract— **Nowadays, Internet of things plays a vital role in all engineering fields and it is a chain of physical devices consolidated with electronic components, software, sensors, actuators and structural connectivity which empowered to the objects to relate and switch the data. The intention is to give security to image transferred through the internet to other devices connected in the common network and it is provided by steganography and additional authentication is done using biometric iris recognition[1]. Data is sent to web server which act as the front end. A device which is also in the network, receives the image which is obscured by steganography and decrypt them to obtain data. The server side programming includes capturing an image by the raspberry pi camera.LSB image steganography is acted on the picture and passed to the server through a webpage. The webpage created is configured to rule the GPIO pins remotely. In the client side, the image is obtained and iris recognition is done[2]. If authenticated then access is given through the webpage and the indication system is used to convey for the user.**

Index Terms—**steganography, security, image, authentication, iris, internet**

I. INTRODUCTION

One faith reasons that trespasser or intruders[1][16] can be recognized is that most of the knowledge they receive from a system is in the form of read and grasp. Intruders may crack the information to others, modify it to confuse an individual or organization, or use it to fire an attack. This can be overcome by using steganography[2][3] and it is a technical approach of masking data in digital media[6]. steganography is one of the energetic techniques to wrap the presence of latent hide data inside a cover object. Photograph are the maximum promoted screen objects for steganography and in this image steganography is adopted[4]. In this, lot of procedure were adopted to lurk information inside cover-image[5].

The spatial domain capacity manages the cover-image pixel bit values to set the cryptic information. The covert bits are written precisely to the mask image pixel bytes. The iris recognition system obtained on an self-regulating bisection system is depends on the change, and can center the circular iris and pupil region, accord eyelids and eyelashes and reflections.

The obtained iris region was then indexed into a rectangular block with no change of dimensionsionality to account for imaging divergence. Finally, from the posture data of 1D Log, Gabor filters are used and sanitized into four levels to encode the uncommon pattern of the iris into a bit-wise biometric template. The hamming distance was employed for differentiation of iris templates, and at last two templates were resulted for comparison.

II. RELATED WORK

In 21st century onwards, IOT techniques has become very popular and getting more meaningful in our day to day life. One of the important thing that need to examine is that, it is the information confidentiality and privacy. The requirement for private and plausible smart environment is vital. In addition, hackers can foray the organization due to the existence of vulnerability within lota and squat processing power devices, that can threaten the privacy of the users. Steganography is a choice to make intimate information and undetectable, hold off hackers from detecting them. With steganography, assailants will not have mindful of information being spread through a channel. Apart from this, researchers are using image steganographic method on many devices for hiding the information or data[13]. In[7], an efficient LSB technique is described as one of the image steganography methods by joannehwan jibe yin, et al. This is because of its less complication compare to complex cryptographic methods as well as high capacity to transfer huge data. A biometric system supplies automatic perception of an individual person based on some set of special feature or characteristics and further it is refined based on various forms like fingerprints, voice, hand geometry, handwriting and the iris.

An efficient biometric method is judged by the use of a particular feature that is highly different so that the probability of any people having the same inherent will be minimal, stable. Moreover, this characteristic does not change over time, and can be easily captured in order to provide improvement to the user thereby preventing the untruth of the feature. The iris is an apparently visible, yet not private organ where one and only autogenetic pattern remains unchanged throughout the human life. These tendency makes very good looking with the use of biometrics[9][10] in classifying the individuals. Image processing techniques[11] are used to combine the one and only iris impression from a digitized image of an eye and encode it into biometric template and can be saved into a database. The resulted figure embrace an objective by producing a mathematical illustration for the one and only information stored in the iris and also permits juxtaposition to be made in between the templates.

When the subject need to be identified by an iris region then this design is then set side by side with the other templates, until the same is found. Libromasek[12] implemented a system which is compressed by a number of subsystems, that corresponds to each level of iris recognition. These stages are segmentation locating the iris and feature encoding and then constructing a template by considering only the most fussy features of the iris. The input will be an gray scale eye image and the output will be an iris template, thereby giving a mathematical representation of the iris region.

III. PROPOSED WORK

The overall actions performed to provide verification and security to image is illustrated. The communication is basically between the client and server and security is provided to image transferred from server to client. The client server model is a common application that severance task are workloads between the source or service, called service, and the service client, called clients. The input to the LSB algorithm[14] for image Steganography is the image taken using the raspberry pi camera[8]. In order for the design procedure to work certain suspicion have been taken. The picture piece is then uploaded to the web server and accessed remotely through internet. Iris recognition is preformed using Integro-differential operator.

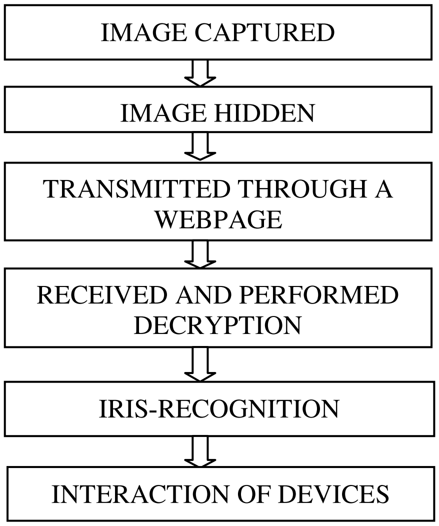


Fig.1. Framework of the workflow

Figure 1 depicts the overall framework and its is divided into the following segments as given below

A) *Image Captured*

The image is nabbed using camera bracketed to raspberry pi and image Steganography is performed in python to veil the image in a carrier image. The Steganographed image is added to the web server and can be picked up remotely from anywhere through the internet[15]· The client the image is downloaded then iris recognition performed to determine authenticity. If the iris matches with the lawful user then access through a button click in website and an LED connected to the pi servers as an indicator.

B) *Transmitted through a Webpage*

PHP,Hypertext Preprocessor server side scripting language introduced primarily for development of webpage and also a general programming language.PHP code may be deep-seated into HTML or HTML% markup or used in consolidated with unalike web design systems, controlling systems and web frameworks.PHP code is manually processed as a common gateway. However the built in library having a large types of imaging conventions and associated inconsistencies.

C) *Iris Recognition*

The iris is the one which is used for regulating the diameter , size of the pupil and the quantity of light arriving the retina. Iris recognition is an self regulated practice of biometric recognition that utilizes mathematical design recognition approaches on taped video images of one or both of the irises of an individual eyes, whose difficult design are unique, stable and can be visualized from distance .The stages in iris recognition are

- localization
- segmentation
- normalization
- template matching

D) *Interaction Of Devices Interfacing Pi With Laptop*

Using the connected HDMI display on pi, VNC server is installed in raspberry pi. LX-Terminal is opened and the commands are used to install VNC.

1. *Interfacing Pi Camera To Raspberry pi*

Raspberry pi camera module is setup by linking the cable into the raspberry pi. The cable channel is preset into the adaptor and placed in between the Ethernet and HDMI ports, with the silver connectors in front of the HDMI port.

2. *Interfacing Indication System*

The indication system is included with led and resistor is connected with raspberry pi through the GPIO pins present in it. GPIO stands for General Purpose Input Output. The circuit consists of power supply and an LED and a resistor. One of the ground pins will act like negative or 0 volts. The positive end of the battery are taken high using pin 18 which means it outputs 3.3 volts, the LED will light.

IV. RESULTS AND DISCUSSION

A) Steganographed Image Generation

The photograph of a person's face is grabbed using a raspberry pi camera connected to the raspberry pi3 which is shown in Figure2(a) and the carrier photograph is taken as in Figure2(b). The captured photography is then hidden in the carrier photograph and the resultant appears in Figure 2(c).

Fig-2(a)captured input image

Fig-2(b)carrier image

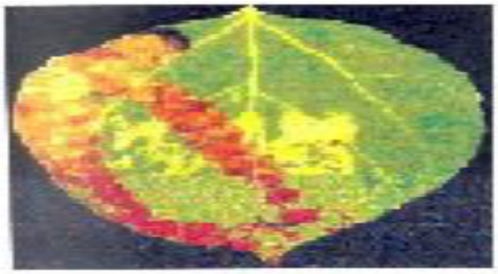
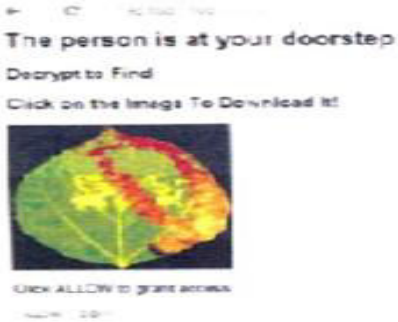


Fig-2(c)hidden image

B) Webpage To Upload Image

The image is then uploaded to the web server through a webpage which is shown in Figure 3.



The person is at your doorstep

Decrypt to Find

Click on the Image To Download it!

Click ALLOW to grant access

Fig.3 Webpage screenshot

C) Retrieving Image

At the receiver side, the client can access the webpage by entering the IP address and downloading the image which is shown in Figure 4(a)

4(a) stegnographed image

4(b)secret image

D)Extracting Of Eye Image-High Solution

The image is obtained and the eye is essenced using viola jones algorithm for both high and low resolution.

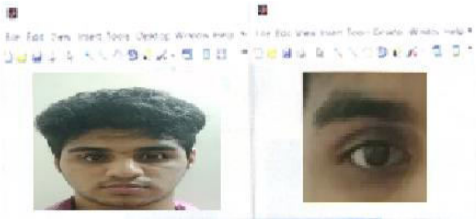


Fig-5(a),5(b):captured input ,extracted eye image

Figure 5(a) is an image obtained and the extracted eye is revealed in Figure 5(b)

E) Extracting of Eye Image-Low Solution

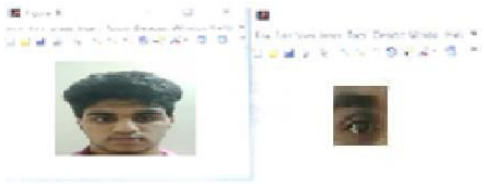


Fig- 6(a), 6(b):captured input image, extracted eye image

Figure 6(a) and 6(b) are the images captured using low resolutions.

F) Iris Recognition

The excerpted eye is then given as input to the recognition system. The recognition is performed in four steps localization, segmentation, normalization, template matching. The steps is dedicated as shown in Figure 7.

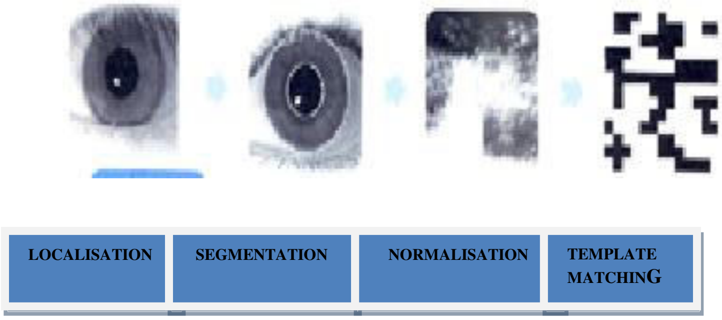


Fig.7 steps involved in iris recognition

The extracted is iris then compared with the image in reference and if both of them matches, access is granted.

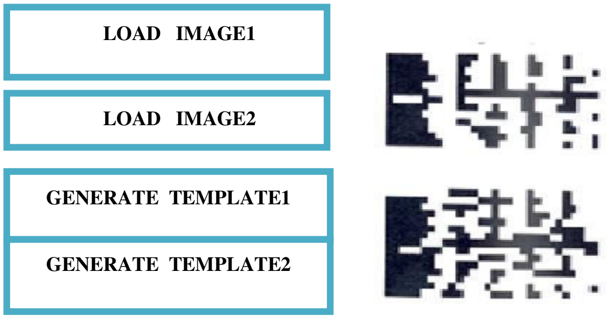


Fig.8. Template matching

Figure 7 shows the template comparison matching between two images.

G) Iris Recognition-Access Granted

If the template is matched access is granted, the LED is given a signal from the GPIO pins of raspberry pi and it glows as shown in Figure 8(a) else the led remains off as shown in Figure 8(b).

Fig-9(a) Led indication to the user-access granted

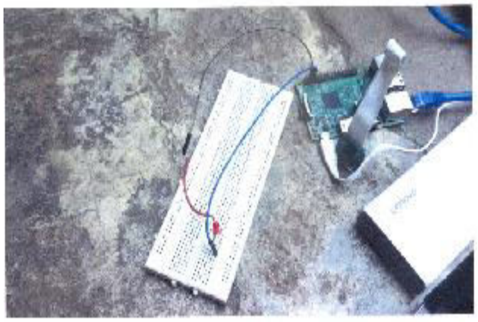


Fig-9(b) Led indiction-access denied

V. CONCLUSION

In today's scenario, Internet of things is a powerful tool to analyze and utilize for information confidentiality and privacy. The needs for protected and trustworthy smart environment is vital. In addition, hackers are able to raid the network due the existence of vulnerability within Iota and low processing power devices, which can threaten the privacy of the users. The image of a person is captured with pi camera connected to raspberry pi and stenography technique using LSB algorithm with a carrier image. It is then uploaded in the web page from the server. The stegnographed image is retrieved from the webpage in the client and connected to the local network. Using LSB algorithm the secret image is unhidden from stegnographed image in python. The secret image is subjected to image processing using MATLAB. The eye region is got from the face image using viola jones algorithm and is given as input to an iris recognition system which performs localization, segmentation, normalization and template matching. The extracted eye image is used to generate a iris code which is then compared with that of the iris code generated for the image of the approved person. If the iris code match then the person is approved by sending high signal from client to server through webpage. Using the GPIO pins the indication system having an LED is made to glow if an high signal is received granting the person to access. Hence iris recognition proves to be an effective way being used as a biometric and LSB stenography proves to provide security needed for communication between IOT devices. The webpage used for accessing is also user-friendly.

REFERENCES

[1] A.W.Atamli and A.Martin,"Threat-Based Security Analysis for the Internet of things(SIoT),2014 International workshop on,2.014,pp.35-43.

[2] R.Wildes. Iris recognition:an spurting biometric technology. Proceedings of the IEEE,vol.85,No.9,1997.

[3] J.Daugman. How iris recognition works. Proceedings of 2002 international conference on image processing,vol.1,2002.

[4] M. Reisslein and B. Rinner, A. Roy-Chowdhury, "Smart camera networks [guest editors ‘ introduction]", *Computer*, vol. 47, no. 5, pp. 23-25, May 2014.

[5] T. Winkler, B. Rinner, "Security and privacy protection in visual sensor networks: A survey", *ACM Comput. Surv.*, vol. 47, no. 1, pp. 2:1-2:42, May 2014

[6] S. P. Mohanty, "A secure digital camera architecture for integrated real-time digital rights management", *Journal of Systems Architecture*, vol. 55, no. 10-12, pp. 468-480, 2009.

[7] N. Tiwari, D. M. Shandilya, "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", *International Journal of Computer Applications*, pp. 0975-8887, 2010.

[8] N. Provos, P. Honeyman, "Hide and seek: An introduction to steganography", *Security & Privacy IEEE*, vol. 1, pp. 32-44, 2003.

[9] B. Lakhsmi, B. V. Raju, "FPGA Implementation of Lifting DWT based LSB Steganography using Micro Blaze Processor", *International Journal of Computer Trends and Technology (IJCTT)*, vol. 6, pp. 6-14, 2013.

[10] T. Winkler, B. Rinner, "Secure embedded visual sensing in end-user applications with TrustEYE.M4", *Proc. IEEE International Conference on Intelligent Sensors Sensor Networks and Information Processing (ISSNIP)*, pp. 1-6, Apr. 2015

[11] M. S. Shahreza, "An improved method for steganography on mobile phone", *WSEAS Transactions on Systems*, vol. 4, pp. 955-957, 2005.

[12] D. Stanescu, V. Stangaciu, I. Ghergulescu, M. Stratulat, "Steganography on embedded devices", *Applied Computational Intelligence and Informatics 2009. SACI'09. 5th International Symposium on*, pp. 313-318, 2009.

[13] C.-K. Chan, L.-M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern recognition*, vol. 37, pp. 469-474, 2004

[14] S. A. Laskar, K. Hemachandran, "High Capacity data hiding using LSB Steganography and Encryption", *International Journal of Database Management Systems (IJDMS)*, vol. 4, 2012.

[15] T. Morkel, J. H. Eloff, M. S. Olivier, "An overview of image steganography", *ISSA*, pp. 1-11, 2005.

[16] A. Westfeld, F5 – A Steganographic Algorithm, In: Moskowitz I.S. (eds) Information Hiding, IH 2001, Lecture Notes in Computer Science, vol 2137. Springer, Berlin, Heidelberg, 2001