International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13325-13335
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

An Enhanced Least Significant Bit Steganography to Improve the Effectiveness of Graphical Password Authentication

Ponmani E, Indhuja S, Puviarasi R, Saravanan Palani*, Ananthakrishnan S
School of Computing, SASTRA Deemed University, India
*Corresponding Author

ABSTRACT
Authentication means acknowledging a user's identity. It is the way of associating a request with a set of identity. The identification provided is an authorized user's information on a personal computer system or within an authentication server. A graphical password is a validation system in which user has to select from images, in a particular order, presented in a graphical user + interface (GUI). Graphical passwords can be easily remembered, as users remember images better than words. Also, the system should be more unaffected by brute-force attacks, because there is practically an infinite search space. Complex text passwords are hard to remember and simple textual passwords are easy to guess. Graphical passwords provide more robustness and memorability. It is a secure mechanism to provide authenticated sign up to a system.
Keywords: Image Steganography, ELSB algorithm, Pattern hiding, Graphical password.

1. INTRODUCTION

Steganography is the technique of invisible Communication. Steganography means one data should be hidden within data. It is an encryption technique and it is combined with Cryptography method as a secure method to protect data. The aim of steganography is to hide the image from hackers. The components of steganography are 1. Cover image 2. Stego key 3.Message. It is shown in Fig.1.

The cover image carries the hidden message. Key is used to encode/decode the message into the message. A message can be anything password, secret data, pattern etc. There are some factors that determine the efficiency of techniques.

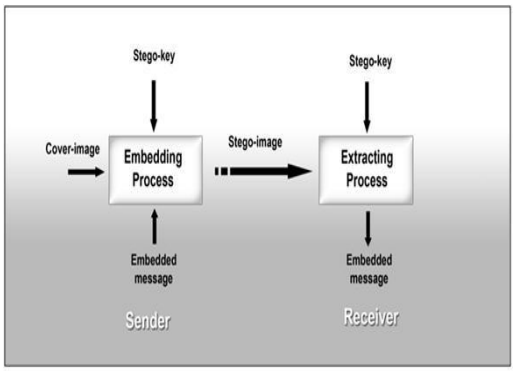

Fig 1: Steganography method for embedding and extracting image.

They are,

1. MSE
2. PSNR
3. SNR.

MSE:

Mean square error. It measures the average of the square of the errors or derivations that is difference between the estimator and what is estimated. The graph is shown in Fig.4.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(y_i - \hat{y}_i\right)^2$$

PSNR:

Peak signal to noise ratio is a proportion of extreme possible power of a signal and power of corrupting noise and that affect the damage of representation. The graph is shown in Fig.5.

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}\left(MAX_I\right) - 10 \cdot \log_{10}\left(MSE\right) \end{aligned}$$

SNR:

Signal noise ratio. It is the measure that compares the level of a desired signal to the level of background noise. It is the ratio of signal power to noise power. The graph is shown in Fig.6.

$$SNR = \frac{P_{signal}}{P_{noise}} = \frac{V_{rms}^2}{V_{qn}^2}$$

$$SNR_{dB} = 10\ log_{10}\left(\frac{P_{signal}}{P_{noise}}\right) = 20\ log_{10}\left(\frac{V_{rms}}{V_{qn}}\right)$$

2. RELATED WORK

Mstafa, R. J. Christian Bach[1] proposed a technique called digital watermarking which is an application of steganography to hide the data within in an image .P.Sumathi, T.Santanam and G.Umamaheswari [2] they classified Steganography methods into six categories, which are substitution technique, Transform domain technique, Spread spectrum technique, Distortion technique. Sumeet Kaur, Savina Bansal, R.K.Bansal [3] they have used some embedding methods which are Spread Spectrum, Masking, Statistical and Distortion Shradha M. Gurav, Leena S. Gawade, Nilesh R. Khochare [4] they proposed cloud with graphical security by means of image password. Er.Aman Kumar, Er.Naveen Bilandi [5] they proposed a method of authentication for mobile phones, ATM machines, E-transactions by graphical passwords. Jeevana, P [6] they proposed cyclomatic method for authentication system. Juneja, K [7] they proposed a graphical password authentication method by XML transformation method. Pavani, M., Naganjaneyulu, S., & Nagaraju, C [8] they proposed a LSB method to embed a text in image. Zhang, T., & Ping, X.[9] they proposed statistical analysis on different image histogram by detecting least significant bit. Ker, A. D. [10] they proposed histogram characteristic function for detecting least significant bit in image for embedding text. Morkel, T., Eloff, J. H., & Olivier, M. S.[11] they proposed image steganography algorithm for hiding text in image. Luo, W., Huang, F., & Huang[12] they proposed Edge image steganography in least significant bit for embedding image. Parvez, M. T., & Gutub [13] they proposed RGB steganography algorithm to store variable number of bit in every channel. Arunkumar S, et.al. [14] have proposed secret image sharing for the set medical images of different size. BrahmaTeja, K. N., Madhumati, D. G., & Rao, K. R. K.[15] they proposed edge steganography for hiding

data in image . In this method they hide the data only in edge.

3. LSB ALGORITHM

The most familiar and popular method of modern day Steganography is to make use of LSB of image pixel data [16-29]. This technique works perfectly when the file is higher than the message file and if an image is grayscale [30-39]. In a grayscale image, every pixel is denoted by eight bits. The pixel last bit is called as Least Significant bit as its value will damage the pixel value only by "1". So, the method is used to keep hidden the information in the image. The LSB steganography is a method of which least significant bit of the image is exchanged with the data bit. As this approach is unsecured to steganography analysis so we can encrypt the raw data before adding it to the image so it will make more secure. This encryption process increases the complexity of time but at the same time, it gives more security. It is the easy approach. In this approach, the LSB of the image is replaced with secret message bit. When applying LSB technique, each byte of a 24-bit image can be encoded into each pixel of three bit. LSB technique may be implemented in specific data area – for example, the frequency coefficients of a JPEG image or embedding a secret message into the RGB bitmap data.LSB technique also implemented to a different data types and formats. Therefore, LSB technique is most important steganography techniques used today. This is depicted in Fig.2.

We can use images to hide things if we replace the last bit of every color's byte with a bit form the message.

Message A-01000001
Image with 3 pixels
Pixel 1:11111000 11001001 00000011
Pixel 2:11111000 11001001 00000011
Pixel 3:11111000 11001001 00000011
Now we hide our message in the image.
Message: 01000001
Pixel 1:11111000 11001001 00000010
Pixel 2:11111000 11001000 00000010
Pixel 3:11111000 11001001 00000011

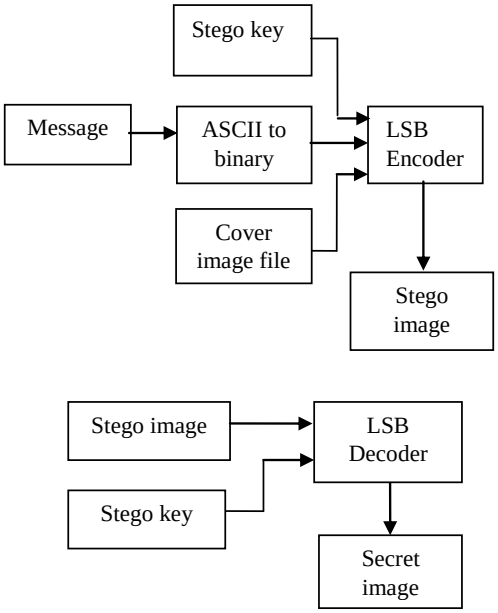

Fig 2. Encoding and decoding of LSB method

4.PROPOSED MODEL

Enhanced Least Significant Bit algorithm. In case of a 24-bit image, LSB algorithm all the three components are used for embedding the hidden message. But in ELSB algorithm only one component among three components (Red, Green, and Blue) can be used to store 3 bits of the secret message. Since only one component is changed we can minimize the distortion

level in the image. Security can be further increased by performing XOR encoding and XOR decoding operations. Main Advantage of Enhanced Least Significant Bit minimizes the distortion level of the image file and security can also be increased.The following digram explain this methods Fig.3.

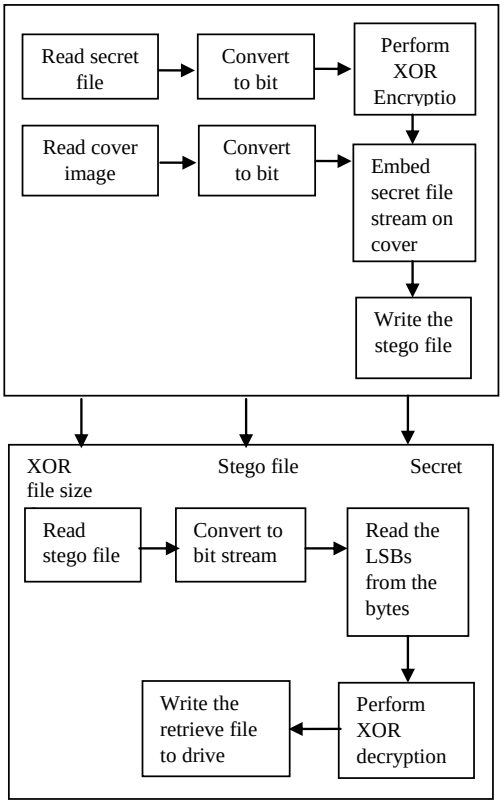

Fig 2. Encoding and decoding of LSB method

5. COMPARATIVE ANALYSIS

ELSB algorithm is more efficient and less distortion when compared to LSB algorithm.LSB algorithm hides the information in the entire three colours of the pixel components distortion will occur due to change in the entire colour hence to overcome this distortion ELSB comes into existence. In LSB algorithm if the pixel of the cover image with the RGB compounded B8B8B8 is used in binary.10111000-10111000-10111000.To hide 111 in the cover image. The result will be 10111001-10111001-10111001 depicted in Table.1.

Table 1. Example for LSB algorithm

	HD	D	R	G	B
Original pixel	B8B8B8	12105912	184	184	184
Modified pixel	B9B9B9	12171705	185	185	185

This LSB algorithm produces some distortion in the pixel. The three LSB bits are changed. In ELSB algorithm if the Pixel of cover image with the RGB compounded B8B8B8 is used in binary.
10111000-10111000-10111000 to hide 111 in the cover image. The result will be 10111000-10111000-10111111depicted in Table.2.

Table 2. Example for ELSB algorithm

	HD	D	R	G	B
Original pixel	B8B8B8	12105912	184	184	184
Modified pixel	B8B8BF	12108919	184	184	191

PSNR value of ELSB is higher than LSB.SNR and MSE value of ELSB is lower than LSB. This shows that ELSB algorithm reduces noise. Comparison is shown in Table.3.

Table 3. Comparison of noise ratio in LSB and ELSB

	PSNR	**SNR**	**MSE**
LSB	20.9015	18.5078	498.0065
ELSB	21.0510	18.4660	497.8213

So, it made an intention to the intruders to hack or demolish the data. In our proposed

system, we are performing a new technology called ELSB for data security; it will not only transform the value of data but also hides the existence of data from the third parties.

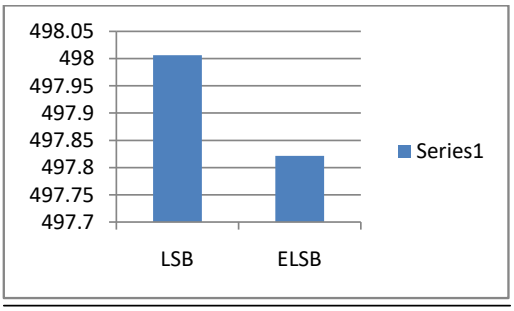

Fig 4: Comparison of LSB and ELSB by MSE value

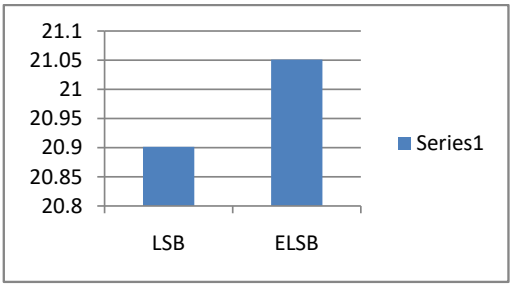

Fig 5: Comparison of LSB and ELSB by PSNR value

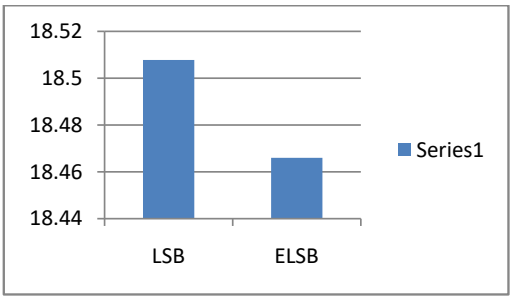

Fig 6: Comparison of LSB and ELSB by SNR value

The main goal of this system is hiding a higher amount of secured data regardless of the size, dimensions of the picture and without disturbing the clarity of the original image. Image-based authentication using steganography is a proposed model which is very helpful to the user in many ways. 1. There is no need for users to remember password only user has to identify the embedded image. 2. The user can retain password secretly in the form of an image. 3. No need for a user to type the password because the user has to browse the image using the mouse. 4. This method prevents social engineering (on password) in user side.

There will be three interfaces as follows,

a. Sign up interface
b. Authentication interface
c. Login interface

6.1. Sign up interface

This is simple and traditional Sign-up interface through which the user can create a new account. The user has to fill all mandatory fields. First time user can easily sign up their account.

6.2. Authentication interface

In this interface, ELSB algorithm is used for embedding pattern in one image. Here, the user has to select one image among given four images and draw the graphical pattern. In our proposed system user has to select at least three points to draw the pattern. That pattern will be embedded into the image using ELSB algorithm. The embedded password image will be stored in the database. It is shown in Fig.7.

6.3. Login interface

There is a very simple login procedure. The user has to provide a username and select a secret image which they have already

selected while they sign up and draw the correct graphical pattern.

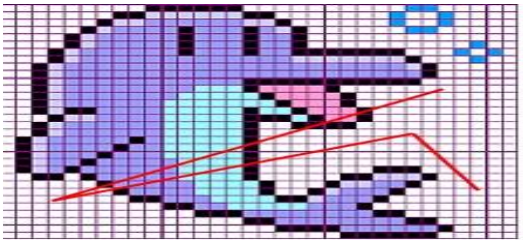

Fig 7: Graphical pattern is embedded in image using ELSB algorithm

When the user submits their detail to the concerned server, username and secret image will silently transmit over the database. If the pattern is correct, it will go to the user account or else pattern mismatch message will be displayed.

7. SUMMARY

In today's world, many authentication systems are there. If they are dividing based on availability and security then most of them will fall into the division of security that ensures the safety of the user's account, but they will lead insufficiency of proper availability. The remaining are the authentication schemes that are intended to reach better availability, but it does not have proper security to secure the user from masqueraded server attacks and communication channel attacks. This examination was aimed at providing authentication schemes that will connect the gap between availability and security. It was also aimed that the security is achieved using a smart card as the second factor whereas the usability using graphical passwords. Graphical Password-based Authentication Scheme: Since usable authentication is an important area of usable security, this research also focused on the usability aspect of the authentication schemes. Most of the existing graphical password based schemes requires verifier table. Therefore, the research objective was to propose a graphical password based Two-Factor Authentication scheme that does not require verifier table. The text password has less security when compared to a graphical password. In graphical passwords, continuous clicks will be created the password. The click events are executed on the different image or on the same image. Or the user can also select particular images which they want to be their graphical password. The Graphical password provides security against the dictionary attacks which is more hazards in web applications. The Graphical password also gives security against the relay attacks.

8. CONCLUSION

A proposed system gives more effectiveness and security. The user can easily remember their password. It is vulnerable to attack. Graphical passwords are better to memorized images than text passwords. Graphical patterns seem to provide a much higher set of usable passwords. For example, people can easily identify the person which he knows from million of faces; Authentication system using this aspect. As another example, a user can choose continuous points in an image as a password; this makes the huge number of probabilities, if the image is more complex and large, and it has good resolution. Graphical passwords have been proposed to

overcome the drawbacks of text passwords. The Proposed system explains that user has to register with the bank using the necessary requirements. While registering, there will be 4 images. A user has to draw a pattern on a particular image and set that as the password. The pattern will be saved on the bank server. The pattern will be embedded on the image using Enhanced LSB technique. User has to login for processing purpose. While login, image and the pattern should be selected. The bank server will cross check the image and the pattern of the user with the registered image and pattern of the user .If the pattern matches, the user can proceed forward for the process. If the pattern mismatches, the user should redraw pattern.

9. REFERENCE

[1] Mstafa, R. J. (2013, March). Information Hiding in Images Using Steganography Techniques. ASEE.

[2] Sumathi, C. P., Santanam, T., & Umamaheswari, G. (2014). A study of various steganographic techniques used for information hiding. arXiv preprint arXiv:1401.5561.

[3] Kaur, S., Bansal, S., & Bansal, R. K. (2014, March). Steganography and classification of image steganography techniques. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 870-875). IEEE.

[4] Gurav, S. M., Gawade, L. S., Rane, P. K., & Khochare, N. R. (2014, January). Graphical password authentication: Cloud securing scheme. In Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on (pp. 479-483). IEEE.

[5] Kumar, E. A., & Bilandi, E. N. (2014). A Graphical Password based Authentication based System for Mobile Devices. International Journal of Computer Science and Mobile Computing, 3(4), 744-754.

[6] Jeevana, P. Evaluation of McCabe's Cyclomatic Complexity Metrics for Secured Medical Image..

[7] Juneja, K. (2017). An XML transformed method to improve effectiveness of graphical password authentication. Journal of King Saud University-Computer and Information Sciences

[8] Pavani, M., Naganjaneyulu, S., & Nagaraju, C. (2013). A survey on LSB based steganography methods. International Journal Of Engineering And Computer Science ISSN, 2319-7242..

[9] Zhang, T., & Ping, X. (2003). A new approach to reliable detection of LSB steganography in natural images. Signal processing, 83(10), 2085-2093.

[10] Ker, A. D. (2005). Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, 12(6), 441-444.

[11] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (pp. 1-11).

[12] Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE transactions on

information forensics and security, 5(2), 201-214.

[13] Parvez, M. T., & Gutub, A. A. A. (2008, December). RGB intensity based variable-bits image steganography. In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 1322-1327). IEEE.

[14] Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., Logesh, R. Meta-data based secret image sharing application for different sized biomedical images (2017) Biomedical Research (India), 2017 (Special Issue), pp. 1-5.

[15] BrahmaTeja, K. N., Madhumati, D. G., & Rao, K. R. K. (2012). Data hiding using EDGE based steganography. International journal of Emerging Technology and advanced Engineering, 2(11), 285-290.

[16] Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Gao, X. Z., & Indragandhi, V. (2017). A hybrid quantum-induced swarm intelligence clustering for the urban trip recommendation in smart city. Future Generation Computer Systems, 83, 653-673.

[17] Subramaniyaswamy, V., & Logesh, R. (2017). Adaptive KNN based Recommender System through Mining of User Preferences. Wireless Personal Communications, 97(2), 2229-2247.

[18] Logesh, R., & Subramaniyaswamy, V. (2017). A Reliable Point of Interest Recommendation based on Trust Relevancy between Users. Wireless Personal Communications, 97(2), 2751-2780.

[19] Logesh, R., & Subramaniyaswamy, V. (2017). Learning Recency and Inferring Associations in Location Based Social Network for Emotion Induced Point-of-Interest Recommendation. Journal of Information Science & Engineering, 33(6), 1629–1647.

[20] Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment Analysis of Tweets for Estimating Criticality and Security of Events. Journal of Organizational and End User Computing (JOEUC), 29(4), 51-71.

[21] Indragandhi, V., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Siarry, P., & Uden, L. (2018). Multi-objective optimization and energy management in renewable based AC/DC microgrid. Computers & Electrical Engineering.

[22] Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2018). An ontology-driven personalized food recommendation in IoT-based healthcare system. The Journal of Supercomputing, 1-33.

[23] Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2018). Hybrid Transform based Adaptive Steganography Scheme using Support Vector Machine for Cloud Storage. Cluster Computing.

[24] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Resources, configurations, and soft computing techniques for power management and control of PV/wind hybrid system. Renewable and Sustainable Energy Reviews, 69, 129-143.

[25] Ravi, L., & Vairavasundaram, S. (2016). A collaborative location based travel recommendation system through enhanced rating prediction for the group of users. Computational intelligence and neuroscience, 2016, Article ID: 1291358.

[26] Logesh, R., Subramaniyaswamy, V., Malathi, D., Senthilselvan, N., Sasikumar, A., & Saravanan, P. (2017). Dynamic particle swarm optimization for personalized recommender system based on electroencephalography feedback. Biomedical Research, 28(13), 5646-5650.

[27] Vairavasundaram, S., Varadharajan, V., Vairavasundaram, I., & Ravi, L. (2015). Data mining-based tag recommendation system: an overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 5(3), 87-112.

[28] Logesh, R., Subramaniyaswamy, V., & Vijayakumar, V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. Electronic Government, an International Journal, 14(1), 90-113.

[29] Vijayakumar, V., Subramaniyaswamy, V., Logesh, R., & Sivapathi, A. (2018). Effective Knowledge Based Recommeder System for Tailored Multiple Point of Interest Recommendation. International Journal of Web Portals.

[30] Subramaniyaswamy, V., Logesh, R., & Indragandhi, V. (2018). Intelligent sports commentary recommendation system for individual cricket players. International Journal of Advanced Intelligence Paradigms, 10(1-2), 103-117.

[31] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Topological review and analysis of DC-DC boost converters. Journal of Engineering Science and Technology, 12 (6), 1541–1567.

[32] Saravanan, P., Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2017). Enhanced web caching using bloom filter for local area networks. International Journal of Mechanical Engineering and Technology, 8(8), 211-217.

[33] Arunkumar, S., Subramaniyaswamy, V., Devika, R., & Logesh, R. (2017). Generating visually meaningful encrypted image using image splitting technique. International Journal of Mechanical Engineering and Technology, 8(8), 361–368.

[34] Subramaniyaswamy, V., Logesh, R., Chandrashekhar, M., Challa, A., & Vijayakumar, V. (2017). A personalised movie recommendation system based on collaborative filtering. International Journal of High Performance Computing and Networking, 10(1-2), 54-63.

[35] Senthilselvan, N., Udaya Sree, N., Medini, T., Subhakari Mounika, G., Subramaniyaswamy, V., Sivaramakrishnan, N., & Logesh, R. (2017). Keyword-aware recommender system based on user demographic attributes. International Journal of Mechanical Engineering and Technology, 8(8), 1466-1476.

[36] Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated Message Filtering System in Online Social Network. Procedia Computer Science, 50, 466-475.

[37] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Unstructured data analysis on big data using map reduce. Procedia Computer Science, 50, 456-465.

[38] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Intelligent travel recommendation system by mining attributes from community contributed photos. Procedia Computer Science, 50, 447-455.

[39] Vairavasundaram, S., & Logesh, R. (2017). Applying Semantic Relations for Automatic Topic Ontology Construction. Developments and Trends in Intelligent Technologies and Smart Systems, 48.