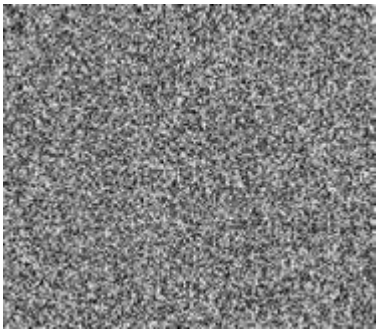
converted grey image. Header file is then read in XPS using system c and after implementing on SPARTAN 3 EDK board we get the results as shown in figure 5.

(a) Input Image



(b) Encrypted Image

(c) Decrypted Image

Figure 5: (a) Input Image (b) Encrypted Image (c) Decrypted Image

4. Conclusion

AES algorithm on FPGA based image encryption and decryption has been proposed in this paper to protect the confidential image data from an unauthorized access. This AES algorithm can process with the data block of 128 bit and cipher key length of 256 bit. Same key is used to encrypt and decrypt the data. The use of 256 bit cipher key to achieve the high security, because 256 bit cipher key is difficult to break. As a result of this secure transmission of image can be possible. Xilinx platform studio (XPS)10.1 with impulse c is used for synthesis of AES algorithm.

References

[1] National Institute of Standards and Technology (NIST), "Data Encryption Standard (DES)," National Technical Information Service VA 22161, 1999.
[2] FIPS 197, "Advanced Encryption Standard (AES)," November 26, 2001.
[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer, Information, Systems and Control Engineering Vol:1 No:3, page 726-731, 2007.
[4] Kamali S.H, Shakerian R, Hedayati M and Rahmani M, "A new modied version of Advanced Encryption Standard based algorithm for image encryption", (ICEIE) International Conference On Electronics and Information Engineering, volume 1, page 1250-1255, Aug 2010.
[5] Ahmad N, Hasan R and Jubadi W.M, "Design of AES S-box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), page 512-517, Oct 2010.
[6] Hoang Trang and Nguyen Van Loi, "An Efficient FPGA Implementation of The Advanced Encryption Standard algorithm", IEEE International Conference on Computing and Communication Technology, page 1-4, Ho Chi Minh city, 2012.
[7] El Maraghy M, Hesham S and Abd El Ghany M.A, "Real-time Efficient FPGA Implementation of AES Algorithm", IEEE International SOC Conference (SOCC), page 203-208, Sept 2013.
[8] M.Sambasiva Reddy and Mr.Y.Amar Babu, "Evaluation Of Microblaze and Implementation Of AES Algorithm using Spartan-3E", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, page 3341-3347, July 2013.